ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL

Facultad de Ingeniería en Electricidad y Computación

"ANÁLISIS DE LA IMPLEMENTACIÓN DE VOIP DE LA RED DE DATOS PERTENECIENTE A LA RED DE COMUNICACIONES DEL COMANDO CONJUNTO DE LAS FUERZAS ARMADAS DEL ECUADOR"

TESIS DE GRADO

Previa a la obtención del Título de:

INGENIERO EN ELECTRÓNICA Y TELECOMUNICACIONES

Presentado por

LUIS HERNÁN CORTEZ HINNAOUI

MARY ELIZABETH LEE OTHON

GUAYAQUIL - ECUADOR

2007

TRIBUNAL DE GRADUACIÓN

Ing. Gustavo Bermúdez
DECANO DE LA FIEC

Ing. Ivonne Martín
DIRECTOR DE TESIS

Ing. César Yépez
VOCAL PRINCIPAL

Ing. Karina Astudillo
VOCAL PRINCIPAL

DECLARACIÓN EXPRESA

"La responsabilidad del contenido de la presente Tesis de Grado nos corresponden exclusivamente, y el patrimonio intelectual de la misma a la ESCUELA SUPERIOR POLITÉCNICA DEL LITORAL"

_____

Luis H. Cortez Hinnaoui

_____

Mary E. Lee Othon

RESUMEN

El Capítulo I describe la situación de la telefonía en el mundo, que en los últimos años ha permitido el surgimiento de otras tecnologías dedicadas a los servicios de comunicaciones. También hacemos un enfoque de la situación telefónica en el Ecuador, haciendo notar que el progreso ha sido mucho más lento a causa de la intervención de los gobiernos y sus intereses políticos, que ha significado un gran perjuicio para los consumidores. En contraste con las comunicaciones en las Fuerzas Armadas que pueden considerarse un servicio un poco más complejo, debido a que éstas además de ser flexibles, escalables y confiables, deben responder rápida y efectivamente a cualquier suceso, brindando un alto nivel de seguridad física contra la posibilidad de ataques enemigos.

El Capítulo II presenta el fundamento teórico necesario para la comprensión y el análisis de la solución de telefonía IP que vamos a proponer. En esta sección se explica una visión de la Red de Telefonía Pública Conmutada, así como el marco teórico detallado de las comunicaciones paquetizadas; para luego presentar las ventajas de telefonía IP sobre la telefonía tradicional.

En el Capítulo III presentamos ante ustedes un camino eficaz, efectivo y eficiente para el desarrollo de nuestro proyecto, que consiste en una metodología, llamada por CISCO PDIOO, misma que cubre las fases de Planificación y Diseño.

El Capítulo IV describe el documento entregado por el usuario, denominado RFP (Request For Proposal), escrito que nos permite visualizar el requerimiento de telefonía IP de las FFAA y que con ayuda de un cuestionario elaborado por nosotros nos dará toda la información necesaria para dar paso a la planificación y diseño de nuestra nueva red.

El Capítulo V ilustra la Fase de Planificación de nuestro proyecto ajustada a las necesidades y características presentadas por los ingenieros encargados de la red de datos de las FF.AA. Hacemos un breve enfoque del backbone y de la calidad de servicio en la WAN y la LAN, así como los servicios que se brindarían.

El Capítulo VI determina los pasos para el diseño de la infraestructura de la red, del procesamiento de llamadas y aplicaciones. Se señala la importancia de la asignación de VLANs para una administración adecuada de la red y la identificación del tráfico con prioridad. La selección de los teléfonos IP y otros equipos para la administración de los procesos de llamadas se establecen de acuerdo a sus capacidades y características y a los requerimientos de los usuarios.

Finalmente se señalan las conclusiones y recomendaciones.

ÍNDICE GENERAL

INDICE DE TABLAS

INDICE DE FIGURAS

1. ANTECEDENTES

1.1 TENDENCIAS TELEFÓNICAS A NIVEL MUNDIAL

En la actualidad, existen empresas que conviven y compiten por el mercado mundial de telefonía fija y celular y para ello, emplean recursos y tecnología de punta con el fin de responder a las necesidades de un mercado de usuarios cada día más exigente.

Con más de 130 años en el mercado, la telefonía fija nació con la idea de haber conseguido la gran solución de comunicación, para el mundo entero. Sin embargo, es difícil creer que hay muchas personas en el mundo que no han hablado nunca por teléfono, y que solamente el 50% de la población mundial tiene acceso a una línea telefónica convencional.

La Figura 1 muestra información acerca de la utilización de la telefonía móvil en el mundo respecto al porcentaje de la población. En algunos países, note que el porcentaje de usuarios móviles supera al tamaño de la población.

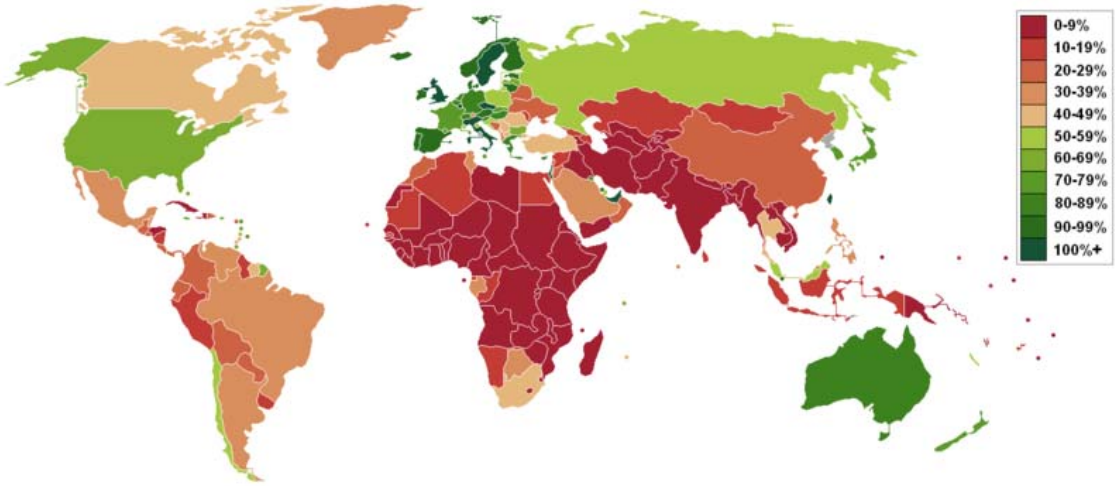

Figura 1. Utilización de telefonía móvil en el mundo (porcentaje de población)

En la actualidad la tendencia mundial es dejar a un lado el teléfono fijo, como una medida para economizar gastos. Hoy, los usuarios prefieren el uso de un teléfono móvil o celular, en vez de pagar el costo de otra línea fija en casa, más la instalación, renta, servicio, entre otros.

En América Latina y África, el avance es más lento porque muchos gobiernos no han realizado nuevas regulaciones en función de las nuevas tendencias en el sector de las telecomunicaciones manteniendo los privilegios y la protección a empresas monopólicas, duopólicas u oligopólicas. Esto ha sido un perjuicio para el consumidor.

Muchas personas que residen en lugares y comunidades lejanas a las que jamás llegó el teléfono fijo han preferido adquirir un celular (generalmente de prepago), a pesar de ello, la recepción no es la mejor en estos sitios o en definitiva existe una falta de señal en sus casas o dentro de sus comunidades. Esta situación pasa a convertirse en un robo y un abuso, porque no puede ofertarse un servicio si la señal no está generalizada para un sector.

Una de las nuevas tendencias que se está presentando en el mundo de las telecomunicaciones es la Voz sobre IP o VoIP; siendo el inicio de una primera etapa de las Redes de Próxima Generación. Por lo expuesto, el valor de la Red de Telefonía Pública Conmutada o PSTN existente puede quedar reducido a cero, a menos que esta red evolucione rápida, eficiente y competitivamente para convertirse en una red de próxima generación.

Es en este momento donde se hace importante entrar a definir VoIP y Telefonía IP, para ello recurrimos a la ITU, Unión Internacional de Telecomunicaciones, que dice:

- **Telefonía IP**, es una parte importante de la convergencia de servicios de datos, teléfonos y televisión en un solo ambiente integrado de información. Telefonía IP es un término empleado para tecnologías que emplean conexiones conmutadas de paquetes bajo el Protocolo Internet, donde se intercambian paquetes de voz, fax, video, u otras formas de información que han sido transportadas en una Red Conmutada de Circuitos.
- **VoIP**, es un término usado en telefonía IP para denotar un conjunto de facilidades que manejan el envió de la información de voz usando el Protocolo

de Internet (IP). En general esto significa enviar información de voz de forma digital en paquetes discretos en vez de los protocolos tradicionales de una red de Conmutación de Circuitos como lo es una PSTN.

Debido a la gran similitud existente en estos 2 conceptos y al modo indiferente en que son empleados por diversos autores, en este trabajo se va a referir también al mismo tiempo como VoIP y Telefonía IP a la infraestructura que permite establecer una llamada telefónica a cualquier tipo de red telefónica existente.

Para los **mercados de escasos recursos** los servicios interactivos - voz, chat, videoconferencia y SMS – son esenciales. En Perú, por ejemplo, el uso de las cabinas públicas está muy difundido entre la población, pero son especialmente importantes para usuarios de bajos ingresos, para los que las cabinas representan la única opción de acceso a Internet. La VoIP es usada ampliamente por todo tipo de usuarios, pero es particularmente apreciada por usuarios de bajos ingresos como se muestra en la Tabla I.

Tabla I. Usuarios de cabinas de VoIP, por estrato socioeconómico (2005)

Estrato socioeconómico	**% de usuarios**
A (superior)	33
B	29
C	29
D/E(inferior)	40
Total de usuarios	33

Se estima que desde el año 2007 al 2012:

- La VoIP y, en general, los protocolos Internet y los servicios de banda ancha se volverán dominantes y determinantes.
- La dominancia de los protocolos IP permite una nueva fase de convergencia en una red única de telecomunicaciones, caracterizada aún por las "redes tontas" (que sólo transmiten) y por "terminales inteligentes" (equipos telefónicos con capacidades de central de conmutación).

  Esto significa que las redes y los protocolos IP son las tecnologías que finalmente han hecho posible la convergencia de todos los servicios de telecomunicaciones en la misma plataforma tecnológica y en las mismas redes.
- En la medida en que las redes IP tienen una arquitectura distinta a la de las redes telefónicas tradicionales, desaparecerán progresivamente las centrales de conmutación y la PSTN.
- Segmentos de negocios como la larga distancia y otros dejarán de ser rentables e irán disminuyendo progresivamente o desaparecerán. La larga distancia es esencial en los ingresos de las empresas telefónicas tradicionales, por lo que es un servicio que no se extinguirá de forma inmediata
- Otra característica de las redes de nueva generación es la tarifa plana de los servicios, que sustituirá al sistema tarifario vigente.
- Las empresas de telecomunicaciones competirán por servicios de valor agregado cada vez más complejos y personalizados para sus clientes
- Se anticipa también una competencia entre las empresas de telecomunicaciones más intensa y puede preverse que será más fuerte ante la entrada de nuevas empresas de VoIP.

- Además se estima que podrían sumarse al servicio de comunicación las empresas eléctricas en la medida en que también entre el 2007 y el 2012 se den avances considerables en la convergencia de las redes de telecomunicaciones y las redes eléctricas (Tecnología PLC).

Es importante señalar la implementación de la telefonía IP en las redes militares, y como ejemplo podemos denotar la participación de la Compañía Cisco Systems, anunciada el 27 de septiembre del 2004. En dicho informe se señala que el Departamento de Defensa de Estados Unidos (DoD) realizó sus pruebas de interoperatividad de su red de VoIP. Además el Joint Interoperability Test Command (JITC) confirmó que todos los aspectos de la solución de Telefonía IP de Cisco cumplen los requerimientos de Interoperabilidad, Confiabilidad, Flexibilidad y Seguridad necesaria para la Defensa de Estados Unidos.

En primera instancia la implementación de VoIP solo se emplearía en las redes administrativas del DoD, pero luego incrementando los niveles de seguridad su uso se dará para el área operativa (Comando y Control de las operaciones netamente militares o durante la guerra).

Para finalizar se estima que aproximadamente desde el 2012 en adelante habrá una segunda etapa en el desarrollo de las redes de nueva generación a nivel mundial, en la que muy posiblemente habrá no sólo "terminales inteligentes", sino "redes inteligentes" de uso civil y militar en todo el mundo y que darán un universo de

posibilidades para servicios de telecomunicaciones cada vez más complejos y de cada vez más alto valor agregado.

1.2 SITUACIÓN DE LA TELEFONÍA EN EL ECUADOR

Para conocer la realidad de la telefonía en el país, haremos un breve resumen del sector en el que se desarrollan las soluciones tecnológicas de este tipo en el país. Por ello en primera instancia podemos decir que el sector de las telecomunicaciones en el Ecuador se compone principalmente de los siguientes organismos: CONATEL, SENATEL Y SUPTEL, cuyas acciones consisten en la Administración, Regulación y Control de las telecomunicaciones:

Cabe señalar que las Fuerzas Armadas o FF.AA. al realizar un proyecto del área de telecomunicaciones establecen que dentro de las fases de análisis y diseño se esté en permanente coordinación con los organismos de control pertinentes a fin de que se brinden los permisos correspondientes tanto en lo referente al espectro a utilizar, como al servicio que se desea brindar.

Considerando el entorno de la telefonía PSTN y de VoIP en el Ecuador, y conociendo que las comunicaciones militares son sin fines de lucro y cuyo único empleo es en beneficio de la Integridad Nacional, las mismas gozan del apoyo de los Organismos de Administración y Control.

En cuanto a la situación de la telefonía IP en el Ecuador, se presenta un escenario diferente a los países desarrollados, ya que los organismos reguladores son parte de un sistema de regulación comprometido con los operadores dominantes. En el Ecuador, las operadoras fijas Andinatel y Pacifictel han estado siendo desafiados por los operadores móviles, como consecuencia del servicio poco satisfactorio que ha caracterizado por algunos años a las empresas de telefonía fija. Además la telefonía móvil ha podido ingresar a mercados rurales en donde la telefonía fija no ha expandido sus redes. Servir estos mercados ha requerido hasta ahora grandes inversiones de baja rentabilidad y alto riesgo. Pocos operadores han penetrado ese mercado, no solo por el riesgo y la baja rentabilidad, sino también por los obstáculos que representa intentar penetrar un mercado débilmente regulado dominado por un operador poderoso.

Las tecnologías inalámbricas y de VoIP están cambiando el cálculo económico de prestación de servicio rural, pero mientras la tecnología cambia, los obstáculos institucionales persisten. Existe un reconocimiento general de que se requieren subsidios gubernamentales para estimular la demanda y la inversión rural. La forma en que estos subsidios se materialicen afectará no solo el servicio a corto plazo, sino la competitividad y el futuro desarrollo de las tecnologías de información y de comunicación en los países en vías de desarrollo.

La telefonía IP en Ecuador no cuenta con una regulación legal definida, centrándose la discusión en aspectos como: *Se trata de Telecomunicaciones o transmisión de*

datos. Respecto a este punto debemos analizar si paga impuestos como el IVA e ICE o no, o *Qué tipo de licencias se requieren para prestar el servicio*.

Las normas legales de formas diversas tratan específicamente de proteger monopolios establecidos por operadoras a menudo ineficientes que encarecen los servicios sin beneficio para el usuario.

En Ecuador se han colocado barreras para impedir el desarrollo de alternativas de telecomunicaciones tratando de evitar que los usuarios se beneficien de los avances de la tecnología y técnicas modernas a pretexto de proteger a las empresas de telecomunicaciones existentes.

La caída de los ingresos provenientes principalmente de comunicaciones de larga distancia no es resultado solamente del uso de la tecnología VoIP sino también es consecuencia del aparecimiento del correo electrónico como alternativa de comunicación instantánea, más barata y accesible. El ingreso que representan las comunicaciones de larga distancia es muy importante para las operadoras fijas en el Ecuador puesto que constituyen el principal rubro de estas empresas. Es por ello que en el país, las empresas de telefonía fija deben innovar y ofrecer servicios similares para que exista libre competencia con las empresas entrantes.

En el mundo de las telecomunicaciones se suelen emplear mecanismos ilegales como el bypass. Dichos actos no pueden justificarse por ninguna razón, pero el caso de la telefonía IP es sustancialmente diferente pues implica un beneficio para el

usuario y resuelve un problema social de importantes repercusiones y bajo el marco de la ley.

Ante su importancia económica y social, sería sensato esperar que los países en vías de desarrollo, como el Ecuador, persiguieran una política agresiva auspiciando el uso de VoIP y tecnologías inalámbricas. En la práctica lo contrario es la norma; la adopción de estas tecnologías se bloquea, especialmente en países donde los monopolios o los cárteles de operadores capturan el proceso regulatorio. Más allá de sus ventajas económicas y sociales, VoIP es importante para el desarrollo de un marco regulatorio sano y competitivo, al facilitar que nuevos operadores puedan desafiar el dominio de operadores dominantes y sus redes fijas.

Es esencial reconocer la importancia de la incorporación de nuevas tecnologías de comunicaciones que permitan el acceso masivo de un servicio de telefonía que en la actualidad llega de manera deficiente a ciertos sectores en el Ecuador. Estas nuevas alternativas tecnológicas permiten también mejorar la competitividad de los servicios y dan posibilidad a los usuarios de servicios más económicos. La decisión de integrar o migrar completamente hacia una solución de telefonía IP permite a largo plazo incrementar el volumen y la seguridad de las llamadas, además incorporan nuevas funcionalidades y se gana flexibilidad.

Las comunicaciones IP son uno de los paradigmas de la actualidad en cuanto a tecnología de información y de comunicaciones. Permite acortar distancias y reducir costos a largo plazo.

La telefonía IP permite la utilización óptima de las redes de datos desplegadas en las empresas. Las Fuerzas Armadas se proyectan también hacia la integración de telefonía paquetizada en la red de datos con la que disponen, permitiendo que las comunicaciones telefónicas puedan llegar a todas los sitios remotos en los que se encuentran ubicados.

1.3 COMUNICACIONES EN LAS FUERZAS ARMADAS

Al hablar de las comunicaciones militares en Ecuador, se está tratando un tema de Seguridad Nacional, y en función de aquello la reserva de mencionar cierta información que es vital para el desarrollo de las actividades militares del país. A pesar de aquello y con el fin de contribuir en el desarrollo de esta tesis se mencionará toda la información técnica necesaria.

Es necesario recordar que desde comienzos de los años ochenta se ha desarrollado una nueva fase del desarrollo tecnológico denominada la “era de la información”, que iniciada en el mercado civil, ha sido fuertemente aprovechada para desarrollos militares. Además los cambios existentes en el campo de la guerra obligan a los mandos militares a tomar decisiones en muy corto tiempo y que estas se transmitan a los centros de operación militar de forma rápida, segura y confiable. Increíblemente la superioridad militar entre los países que poseen Fuerzas Armadas con bajo presupuesto se da solo con excelentes líneas de comunicación. Asimismo, los medios de comunicación han acercado la guerra a todos los rincones del globo.

Un sistema de comunicaciones moderno debe permitir transportar datos que lleguen a cualquier tipo de dispositivo Terminal que dé facilidades para comandar, controlar, comunicar, inteligenciar, vigilar y reconocer objetivos militares. Sin embargo, la esencia no es la adopción de estos equipos, sino lo que el Almirante Owens (militar norteamericano que impulsó el cambio más significativo en los requerimientos de sistemas para operaciones militares) denomina *sistema de sistemas*, es decir, la acción conjunta de todos los equipos.

El enfoque del *sistema de sistemas* está fijado en la aplicación de técnicas de la información a la guerra, con vistas a integrar las tecnologías existentes y emergentes que puedan *ver, disparar y comunicarse.* Es este último aspecto de interés para esta tesis, ya que al rediseñar la Red de Comunicaciones integrando eficientemente los equipos se podrá lograr el dominio de la Información en tiempos de paz y/o de guerra.

Como puede evidenciarse, una nueva tecnología (VoIP) y una adecuada integración supone una transformación radical de los tradicionales sistemas de comunicación existentes. Por ello un Sistema de Comunicaciones Moderno de las Fuerzas Armadas debe responder de forma rápida y efectiva a cualquier contingencia. Debe poseer una arquitectura de red segura y abierta que facilitará el desarrollo de revolucionarias innovaciones en las capacidades conjuntas.

Los componentes principales del Sistema de Comunicaciones que está operativo en Fuerzas Armadas son:

- Una red de comunicaciones conjunta con una adecuada resistencia y flexibilidad para transmitir rápidamente la información a las fuerzas.
- Un sistema de defensa de los sistemas de comunicaciones propios contra ataques o interferencias de enemigos.

El nivel de seguridad físico que se brinde a la Red de Comunicaciones viene determinado en gran medida por la clasificación de la información que introducirá en él. Un sistema que trabaje únicamente con información no clasificada, podrá tener un bajo nivel de seguridad. En el diseño y ampliación de dicho sistema se sigue como objetivo prioritario la estabilidad y eficacia del mismo.

La información se ha convertido en un producto principal de la guerra moderna. Ya en el pasado, la criptografía, los artificios, la manipulación y la destrucción han sido disciplinas destinadas a las comunicaciones militares. En el futuro, al aumentar la explosión mundial de los sistemas de información comercial, las fuerzas militares pueden emplear sistemas comerciales como satelitales o el mismo Internet para el desarrollo de sus comunicaciones y el transporte de la Información.

Lograr el dominio en la batalla de la información requiere conseguir la ventaja tecnológica y de organización sobre el adversario, lo cual supone tener superioridad a la hora de obtener, procesar y diseminar el flujo ininterrumpido de información, a la vez que se deniega esa facultad al adversario, teniendo en cuenta que la guerra de información es tanto ofensiva como defensiva.

La rapidez con que se suceden las nuevas tecnologías conlleva su pronta obsolescencia, lo que obliga a establecer un compromiso en la modernización/renovación de los equipos de comunicación, agotando al máximo los ciclos de vida o modernizar/sustituir, aplicando las tecnologías más avanzadas.

Como conclusión, se puede decir que un sistema de comunicación moderno ofrece el potencial de emplear a las fuerzas militares con la mayor eficacia posible. Tanto es así, que al poseer Comunicaciones permanentes y seguras podríamos decir *que hemos logrado multiplicar nuestra Fuerza*.

2. MARCO TEÓRICO: RED DE TELEFONÍA PÚBLICA CONMUTADA PSTN Y VOZ SOBRE IP VOIP

2.1 BASES DE LA RED DE TELEFONÍA PÚBLICA CONMUTADA O PSTN

La PSTN es una red con conmutación de circuitos tradicional optimizada para comunicaciones de voz en tiempo real. Cuando llama a alguien, cierra un conmutador al marcar y establece así un circuito con el receptor de la llamada. La PSTN garantiza la Calidad de Servicio o QoS al dedicar el circuito a la llamada hasta que se cuelga el teléfono. Independientemente de si los participantes en la llamada están hablando o en silencio, seguirán utilizando el mismo circuito mientras dure la llamada.

Al mencionar la **Señalización analógica,** la voz humana tiene una forma analógica.

La comunicación analógica no es robusta ni eficaz ante el ruido de línea que se produce por la introducción de interferencias en una red de voz. En los inicios de la red de telefonía, la transmisión analógica se pasaba a través de amplificadores para aumentar la señal. Este método no solo amplificaba la voz, sino también el ruido de línea, provocando a menudo que la conexión fuera inutilizable.

Las señales analógicas que reciben el ruido de línea pueden distorsionar la forma de onda analógica y producir una recepción desvirtuada. La Figura 2 muestra que un amplificador no limpia la señal que amplifica, sino que amplifica la señal distorsionada. Este proceso de pasar por varios amplificadores con una señal de voz se llama ruido acumulado.

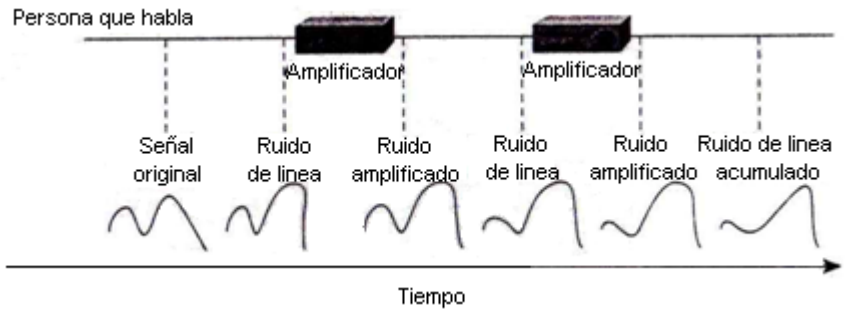

Figura 2. Distorsión de línea analógica

En redes digitales, el ruido de línea no es un problema ya que los repetidores no solo amplifican la señal, sino que también la limpian hasta devolverla a su condición original. Esto es posible con la comunicación digital porque dicha comunicación está basada en *unos* y *ceros*. Por tanto, como muestra la Figura 3, el repetidor (amplificador digital) solo ha de decidir si tiene que regenerar un 1 o un 0.

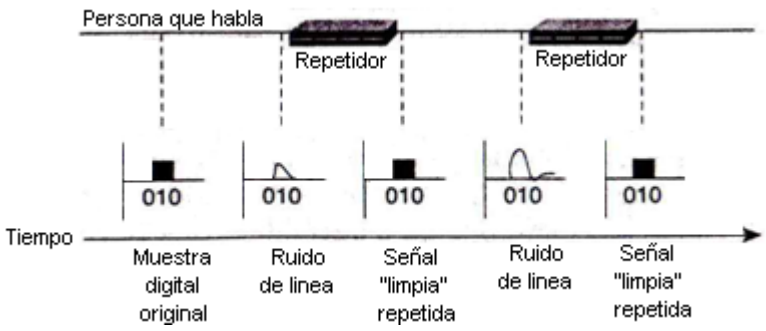

Figura 3. Distorsión de línea digital

Por lo tanto, cuando se repiten las señales, se mantiene un sonido limpio. Cuando los beneficios de esta representación digital se hicieron evidentes, la red de telefonía migró a la modulación PCM que se explica en la sección 2.4.5 .

Generalmente funcionan dos tipos de *métodos de señalización PSTN* sobre varios medios de transmisión. Los métodos de señalización están divididos en los siguientes grupos:

- **Señalización usuario a red.** Es la comunicación entre usuario final y la PSTN. Generalmente cuando utiliza un par de cobre trenzado para el transporte, el usuario se conecta con la PSTN a través de una Red Digital de Servicios Integrados o ISDN analógica, o a través de un carrier T1 (de capa digital 1).

  El método de señalización más habitual para la comunicación analógica usuario a red es la *marcación multifrecuencia (DTMF).* La DTMF se conoce como señalización dentro de banda debido a que los tonos son transportados a través de la ruta de voz. La ISDN utiliza otro método de señalización conocido como *fuera de banda.* Con este método, la señalización es transportada en un canal separado de la voz. El canal en el que la voz es transportada se llama canal

portador (bearer, o canal B) y es de 64 kbps. El canal en el que se transporta la señal se llama canal de datos (o canal D) y es de 16 kbps. La Figura 4 muestra una interfaz de acceso básico que consta de dos canales B y un canal D.

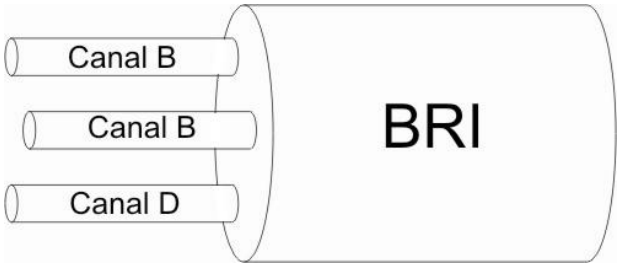

Figura 4. Interfaz de acceso básico

La señalización fuera de banda ofrece muchos beneficios, como reducción de colisión, mayor ancho de banda, etc.

- **Señalización red a red.** Es la manera cómo se intercomunica la PSTN. Normalmente, se lleva a cabo a través de los siguientes medios de transmisión:
  - Carrier T1/E1 sobre par trenzado
  - Carrier T3/E3, T4 sobre cable coaxial
  - Carrier T3, T4 sobre enlace de microondas
  - La Red Optica Síncrona (SONET) a través de los medios de fibra óptica.

Los tipos de señalización red a red incluyen métodos de señalización dentro de banda, como la multifrecuencia (MF) y la señalización de bit robado. Estos tipos de señalización también se pueden utilizar para métodos de señalización de red. La señalización red a red también utiliza un método de señalización fuera de banda conocido como Sistema de señalización 7 (C7 en los países europeos).

2.2 SISTEMA DE SEÑALIZACIÓN 7 o SS7

El SS7 se utiliza para realizar señalización fuera de banda en la PSTN. Soporta la PSTN manejando el establecimiento de la llamada, el intercambio de información, el enrutamiento, las operaciones, la facturación y el soporte para servicios de red inteligente. El protocolo SS7 es importante en VoIP por la manera en que interactúa con la PSTN. Proporciona un protocolo común para la señalización, el envío de mensajes o la definición de interfases para los que se pueden desarrollar dispositivos VoIP.

Este tipo de señalización es una manera por la cual los elementos de la red telefónica intercambian información en forma de mensajes. Los mensajes SS7 pueden transportar información como la siguiente:

- Alguien acaba de discar 593-4-6007451. ¿A dónde enruto la llamada?
- El suscriptor llamado en el tronco 11 está ocupado. Libere la llamada y active un tono de ocupado.
- La ruta hacia XXX está congestionada. Por favor, no envíe ningún mensaje hacia XXX a menos que sean de prioridad 2 o mayor.
- Estoy haciendo que el tronco 143 esté fuera de servicio por mantenimiento.

La red SS7 es un conjunto interconectado de elementos que es utilizado para intercambiar mensajes en soporte de las funciones de telecomunicaciones. El protocolo SS7 está diseñado para facilitar estas funciones y mantener la red en funcionamiento. Como la mayoría de protocolos modernos, el protocolo SS7 está formado por capas.

Estos niveles difieren ligeramente del modelo de referencia OSI. La Figura 5 presenta una comparación entre los niveles del protocolo SS7 y las capas del modelo OSI. Como se puede ver, el protocolo SS7 solo tiene cuatro niveles y el modelo OSI tiene siete. Los niveles 1 al 3 de SS7 (L1-L3) son idénticos a las capas L1-L3 de OSI y el nivel 4 (L4) de SS7 corresponde a las capas 4 a la 7 (L4-L7) de OSI.

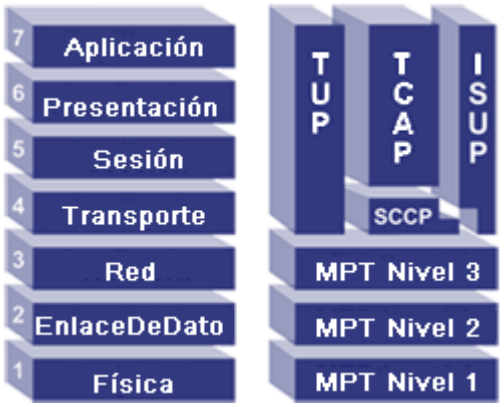

Figura 5. Comparación modelo OSI vs. SS7

El mundo de las comunicaciones se está proyectando a la integración de la telefonía de paquetes y la red SS7 de manera que la tecnología de paquetes de voz pueda ser un verdadero avance en las nuevas redes. En esta sección se ha descrito rápidamente la señalización SS7 para tener la percepción de cómo opera la telefonía tradicional y comenzar el estudio de la telefonía IP.

2.3 PROTOCOLOS DE CONTROL DE LLAMADA VOZ SOBRE IP

Los principales protocolos de control de llamadas VoIP son H.323, el Protocolo de control de gateway simple (SGCP, Simple Gateway Control Protocol), el Protocolo de control de dispositivo del protocolo de Internet (IPDC, Internet Protocol Device Control), el Protocolo MGCP (Media Gateway Control Protocol) y el SIP (Protocolo de Inicio de la Sesión).

2.3.1 PROTOCOLO DE SEÑALIZACIÓN H.323

H.323 es una especificación de la ITU-T para la transmisión de audio, vídeo y datos a través de una red de Protocolo Internet (IP), incluida la propia Internet. El estándar H.323 dirige la señalización, control de llamadas, transporte, control multimedia y control de ancho de banda para conferencias punto a punto y multipunto. Las recomendaciones especifica H.320 para la ISDN y H.324 para la PSTN como mecanismos de transporte.

El H.323 consta de los componentes y protocolos que señala la Tabla II.

Tabla II. Funciones y Protocolos H.323

Función	**Protocolo**
Señalización de llamadas	H.225
Control de medios	H.245
Codecs de audio	G.711, G.722, G.723, G.728, G.729
Codecs de video	H.261, H.263
Compartir datos	T.120
Transporte de medios	RTP/RTCP

El sistema H.323 se explica en las dos siguientes secciones:

2.3.1.1 Elementos H.323

La Figura 6 ilustra los elementos de un sistema H.323. Estos elementos incluyen terminales, gateways GW, gatekeepers GK y unidades de control multipunto (MCU, Multipoint Control Units). Los terminales, a los que a menudo se hace referencia como puntos finales, proporcionan conferencias punto a punto y multipunto para audio, y de manera opcional, video y datos. Los gateways interconectan al punto final de H.323 con la Red pública de telefonía conmutada (PSTN) o la red ISDN (RDSI). Los gatekeepers proporcionan el control de admisión y servicios de traducción de direcciones para terminales o gateways. Las MCU son dispositivos que permiten que dos o más terminales o gateways realicen conferencias con sesiones de audio y/o vídeo.

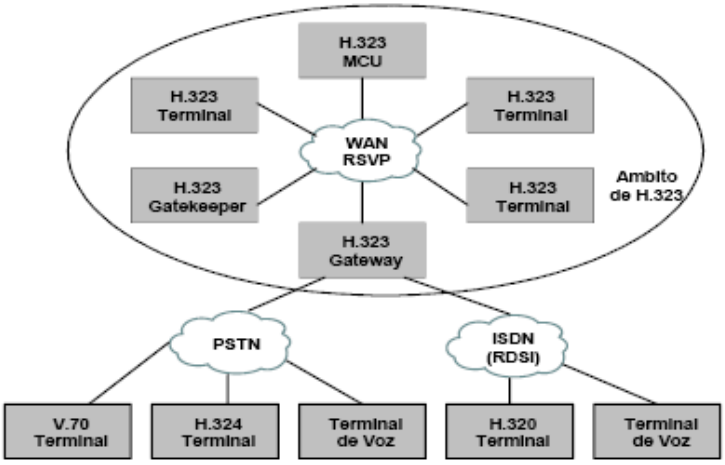

Figura 6. Elementos de networking de H.323

El elemento de red que ilustra la Figura 7 está definido en H.323 como un **terminal.**

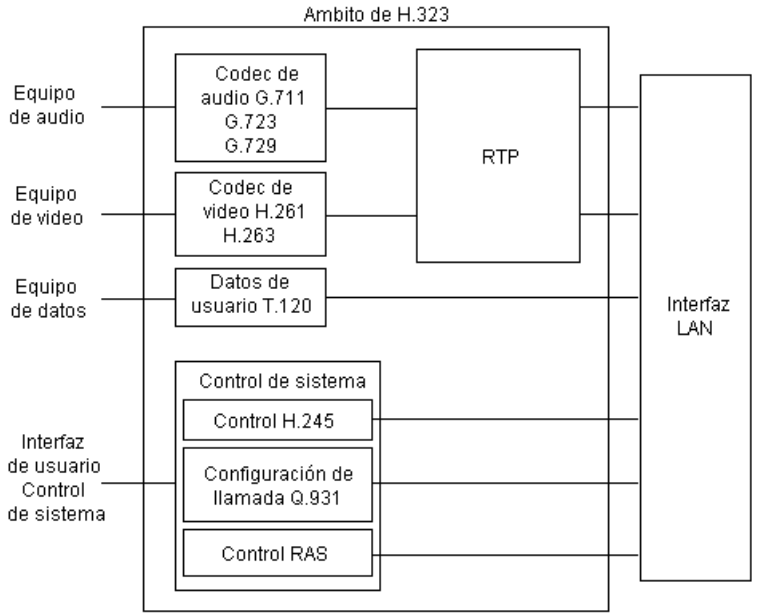

Figura 7. Relaciones entre los componentes de H.323

2.3.1.1.1 Terminales H.323

Los terminales H.323 deben tener una unidad de control de sistema, una transmisión de medios, codec de audio e interfaz de red basada en paquetes. Los requisitos opcionales incluyen un codec de video y aplicaciones de datos de usuario.

Las siguientes funciones y posibilidades se encuentran dentro del ámbito del terminal H.323:

- Unidad de control de sistema

- Transmisión de medios
- Codec de audio
- Interfaz de red
- Canal de datos

2.3.1.1.2 Gateway H.323

El gateway H.323 refleja las características de un punto final de una red de circuito conmutado (PSTN) y un punto final H.323. Traduce entre formatos de audio, vídeo y transmisión de datos, así como en sistemas de comunicación y protocolos. Esto incluye la configuración y el borrado de la llamada en la red IP y en la red PSTN.

Los gateways no son necesarios a menos que se requiera la interconexión con la PSTN. Por tanto, los puntos finales H.323 pueden comunicar directamente sobre la red de paquetes sin conectar con un gateway.

2.3.1.1.3 Gatekeeper H.323

El gatekeeper es una función opcional que proporciona servicios de control de pre-llamada y nivel de llamada a los puntos finales H.323. Los gatekeepers están lógicamente

separados de los demás elementos de la red en los entornos H.323.

Si un gatekeeper está presente en un sistema H.323, debe llevar a cabo lo siguiente:

- Conversión de direcciones.
- Control de admisiones
- Control de ancho de banda
- Administración de zona

Opcionalmente, el gatekeeper puede aportar las siguientes funcionalidades: autorización de llamada, administración de ancho de banda y administración de llamada.

2.3.1.1.4 Controlador multipunto

El controlador multipunto (MC) soporta conferencias entre tres o más puntos finales en una conferencia multipunto. Los MC transmiten el conjunto de capacidades para cada punto final en la conferencia multipunto y pueden revisar las capacidades durante la conferencia. La función MC puede residir en una Terminal, gateway, gatekeeper o MCU.

2.3.1.1.5 Servidor Proxy H.323

Un servidor Proxy H.323 es un Proxy específicamente diseñado para el protocolo H.323. El Proxy actúa en la capa de aplicación y puede examinar los paquetes entre dos aplicaciones que se comunican. Los Proxies pueden determinar el destino de una llamada y realizar la conexión si se desea.

2.3.1.2 Conjunto del protocolo H.323

El conjunto del protocolo H.323 está basado en varios protocolos, como muestra la Figura 8. La familia de protocolos soporta la admisión de llamadas, la preparación, el estado, el borrado, los flujos de medios y los mensajes en los sistemas H.323. Estos protocolos son soportados por mecanismos de entrega de paquetes seguros y poco seguros sobre las redes de datos.

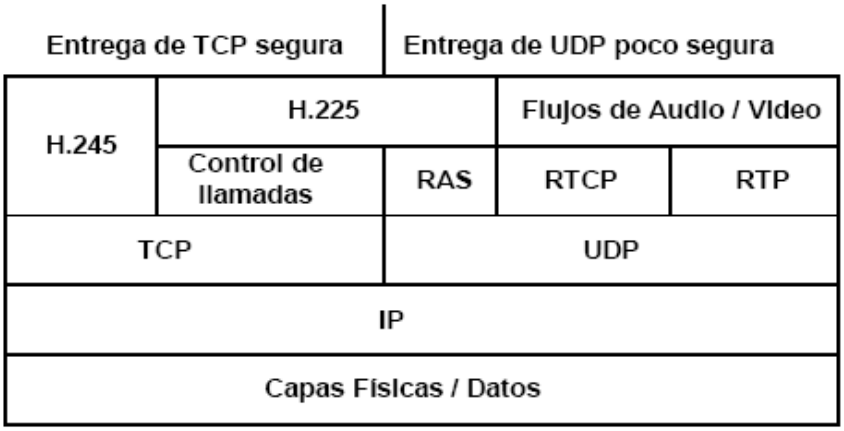

Figura 8. Capas del conjunto del protocolo H.323

El conjunto del protocolo H.323 está dividido en tres áreas de control principales que se explican a continuación.

2.3.1.2.1 Señalización de Registro, Admisiones y Estado

La *señalización RAS* proporciona un control de prellamadas en las redes H.323 donde existen gatekeepers y una zona. El canal RAS se establece entre puntos finales y gatekeepers a través de una red IP. El canal RAS está abierto antes de que ningún otro canal sea establecido, y es independiente de la señalización de control de llamadas y de los canales de transporte de medios. Esta conexión UDP transporta los mensajes RAS que realizan el registro, las admisiones, los cambios del ancho de banda, el estado y los procedimientos de desenganche.

El *descubrimiento del gatekeeper* es un proceso manual o automático que los puntos finales utilizan para identificar con qué gatekeeper registrarse. En el método manual, los puntos se registran directamente con la dirección IP del gatekeeper. El método automático permite que la relación entre puntos finales y gatekeepers cambie a lo largo del tiempo y requiere un mecanismo conocido como *autodescubrimiento.*

El registro es el proceso que permite que los gateways, puntos finales y MCU alcancen una zona e informen al gatekeeper de sus direcciones IP y alias.

Los mensajes de admisión entre puntos finales y gatekeepers proporcionan las bases para la admisión de llamadas y control de ancho de banda.

El control de ancho de banda se administra inicialmente a través del intercambio de admisiones entre un punto final y el gatekeeper.

2.3.1.2.2 Señalización de Control de Llamadas

En las redes H.323, los procedimientos de *control de llamadas se basan en la recomendación H.225*, que especifica la utilización y soporte de los mensajes de señalización Q.931. Un canal de control de llamadas seguro se crea en una red IP en el puerto 1720 del TCP. Este puerto inicializa los mensajes de control de llamadas Q.931 entre dos puntos finales para el propósito de conectar, mantener y desconectar las llamadas.

2.3.1.2.3 Control y Transporte de medios

En el *control y transporte de medios, H.245* maneja mensajes de control de extremo a extremo entre entidades H.323. Los procedimientos H.245 establecen canales lógicos para la transmisión de información de audio, vídeo, datos y canal de control.

Es importante mencionar que, *RTP* proporciona *transporte de medios* en H.323; de manera más específica, RTP permite la entrega de extremo a extremo en tiempo real de audio, vídeo y datos interactivos sobre la red. Los servicios de transmisión y empaquetamiento incluyen la identificación de carga útil, la secuenciación, la marca de temporización y la monitorización. RTP depende de otros mecanismos y de las capas bajas para asegurar la entrega a tiempo, la reserva de recursos, la fiabilidad y la QoS. RTCP monitoriza la entrega de datos y controla e identifica los servicios.

2.3.2 PROTOCOLO DE INICIO DE LA SESIÓN

El Protocolo de inicio de la sesión (SIP) es un protocolo de control de señalización de la capa de aplicación que se utiliza para establecer, mantener y terminar sesiones multimedia. Las sesiones multimedia incluyen la telefonía,

Internet, las conferencias y otras aplicaciones similares que proporcionan medios como audio, video y datos.

Se pueden utilizar invitaciones SIP para establecer sesiones y transportar descripciones de la sesión. SIP soporta sesiones unidifusión y multidifusión, así como llamadas punto a punto y multipunto. Las comunicaciones se pueden establecer y terminar utilizando esas cinco facetas de SIP: localización de usuario, capacidad de usuario, disponibilidad de usuario, configuración de la llamada y manejo de la llamada.

SIP es un protocolo basado en texto que es parte de la arquitectura multimedia general del Grupo IETF (Internet Engineering Task Force). El IETF incluye el Protocolo de reserva de recursos (RSVP, Resouce Reservation Protocol), el Protocolo de transporte en tiempo real (RTP, Real-Time Transport Protocol), el Protocolo de streaming en tiempo real (RTSP, Real-Time Streaming Protocol), el Protocolo de descripción de la sesión (SAP, Session Announcement Protocol) y el Protocolo de descripción de la sesión (SDP, Session Description Protocol). Sin embargo, las funciones SIP son independientes, por lo que no dependen de ninguno de estos protocolos. SIP puede operar en conjunción con otros protocolos de señalización como el H.323. La flexibilidad de SIP permite que servicios telefónicos avanzados y movilidad.

Los dos componentes de un sistema SIP son los **agentes de usuario** y los **servidores de red**. Las partes que llaman y son llamadas se identifican con

direcciones SIP; las partes necesitan localizar **servidores** y **usuarios**. Las **transacciones SIP** también se explicarán en esta sección.

2.3.2.1 Agentes de usuario

Los Agentes de usuario son aplicaciones cliente de sistema final que contienen un cliente usuario-agente (UAC) y un servidor usuario-agente (UAS), también conocidos como *cliente y servidor*, respectivamente.

Un cliente inicia las peticiones SIP y actúa como agente usuario del llamante. El servidor recibe las peticiones y devuelve las respuestas en nombre del usuario; actúa como el agente de usuario llamado.

2.3.2.2 Servidores de red

Existen dos tipos de Servidores de red SIP: los servidores Proxy y los servidores Redirect (redirección). El *servidor Proxy* actúa en nombre de otros clientes y contiene funciones de cliente y de servidor. El *servidor de redirección* acepta peticiones SIP y envía una respuesta redirigida al cliente que contiene la dirección del siguiente servidor.

2.3.2.3 Direccionamiento SIP

Las *direcciones SIP*, también llamadas localizadores universales de recursos (URL) SIP, existen en la forma de usuario@host, similar a

una dirección de correo electrónico. Respecto a la localización de un servidor, un cliente puede enviar una petición SIP directamente a un servidor Proxy configurado localmente, o bien la dirección IP y puerto del correspondiente URL SIP.

2.3.2.4 Transacciones SIP

Cuando se ha resuelto el tema de la dirección, el cliente envía una o más peticiones SIP y recibe una o más respuestas desde el servidor especificado. Todas las peticiones y respuestas asociadas con esa actividad están consideradas como parte de una transacción SIP.

La parte llamada puede desplazarse desde uno a varios sistemas finales a lo largo del tiempo. Puede moverse desde la red de área local (LAN) corporativa a una oficina en casa conectada a un ISP o a una conexión pública Internet mientras atiende a una conferencia. Por tanto, para los **servicios de localización**, SIP necesita acomodar la flexibilidad y la movilidad de los sistemas finales IP. Las localizaciones de estos sistemas finales pueden estar registradas con el servidor SIP o con otros servidores de localización fuera del ámbito de SIP.

La acción y resultado de localizar a un usuario depende del tipo de servidor SIP que se esté utilizando. Un servidor de redirección simplemente devuelve la lista completa de localizaciones y permite

que el cliente localice directamente al usuario. Un servidor Proxy puede probar las direcciones en paralelo hasta que la llamada tenga éxito.

Las **peticiones SIP** son caracterizadas por la línea inicial del mensaje, llamada Request-Line, que contiene el nombre del método, el identificador del destinatario de la petición (Request-URL) y la versión del protocolo SIP. Existen seis métodos básicos SIP (definidos en RFC 254) que describen las peticiones de los clientes:

- **INVITE**: Permite invitar un usuario o servicio para participar en una sesión o para modificar parámetros en una sesión ya existente.
- **ACK**: Confirma el establecimiento de una sesión.
- **OPTION**: Solicita información sobre las capacidades de un servidor.
- **BYE**: Indica la terminación de una sesión.
- **CANCEL**: Cancela una petición pendiente.
- **REGISTER**: Registrar al User Agent.

Después de la recepción e interpretación del mensaje de solicitud SIP, el receptor del mismo da respuesta a mensajes. Este mensaje, es similar al anterior, difiriendo en la línea inicial, llamada Status-Line, que contiene la versión de SIP, el código de la respuesta (Status-Code) y una pequeña descripción (Reason-Phrase).

2.3.3 PROTOCOLO DE SEÑALIZACIÓN MGCP

Otro protocolo competidor con H.323 y SIP es MGCP (Media Gateway Control Protocol). El MGCP es un protocolo que soporta un control de señalización de llamada escalable. El control de calidad de servicio QoS se integra en el gateway GW o en el controlador de llamadas MGC. El MGC realiza el control de procesamiento con la red pública PSTN. El MGC es un software que contiene en su interior al GK. Realiza las siguientes funciones:

- Control de llamada (asimilable al punto de conmutación en las PABX);
- Identificación del tráfico H.323 y aplicación de las políticas apropiadas;
- Limitación del tráfico H.323 sobre la LAN y WAN;
- Entrega archivos **CDR** (*Call Detail Records*) para la facturación (*Billing*);
- Realiza la interfaz con las redes inteligentes;
- Inserta calidad de servicio e implementa políticas de seguridad.

La Figura 9 ilustra el proceso de comunicación entre dominios con el GW.

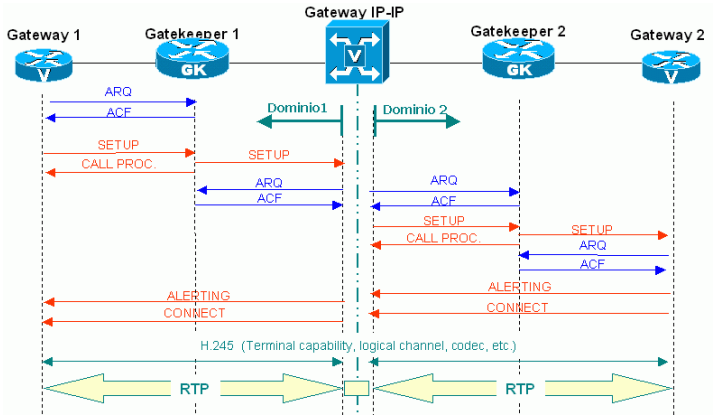

Figura 9. Proceso de comunicación entre dominios con el GW IP-IP

El MGCP es un protocolo que permite comunicar al controlador de gateway MGC (también conocido como *Call Agent*) con las gateway GW de telefonía (hacia la PSTN). Los mensajes MGCP viajan sobre UDP/IP, por la misma red de transporte IP con seguridad IPsec.

El formato de trabajo genera una inteligencia externa a la red (concentrada en el MGC) y donde la red de conmutación está formada por los router de la red IP. El GW solo realiza funciones de conversión vocal (analógica o de velocidad digital) y genera un camino RTP entre extremos. La sesión de MGCP puede ser punto-a-punto o multipunto. El protocolo MGCP entrega al GW la dirección IP, el port de UDP y los perfiles de RPT.

2.3.3.1 Comandos disponibles de MGCP

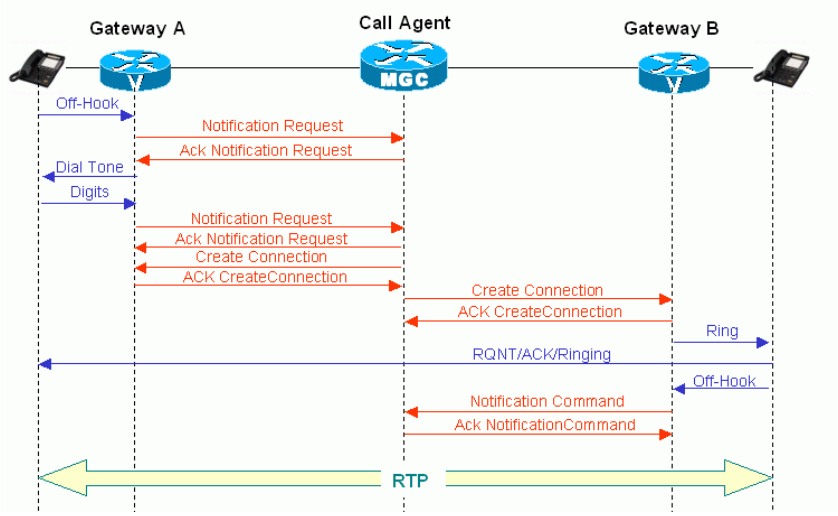

Figura 10. Proceso de comunicación con protocolo MGCP

En la Figura 10 se muestra el intercambio de mensajes en el establecimiento de una comunicación con protocolo MGCP. Los mensajes o comandos disponibles en MGCP son los siguientes:

- NotificationRequest, este primer mensaje se genera ante el requerimiento de conexión de un teléfono. El GW-A indica al MGC el requerimiento del usuario A. Como respuesta se recibe un Ack-NotificationRequest. El mismo comando transfiere los dígitos discados cuando el usuario termina la marcación correspondiente.
- CreateConnection, utilizado para crear una conexión que se inicia en el GW. Se envía a ambos GW y se recibe el comando de confirmación Ack-CreateConnection.
- ModifyConnection, puede ser usado para cambiar los parámetros de la conexión existente.
- DeleteConnection, usado para cancelar la conexión existente al final de la llamada.
- AuditConnection, usado para requerir el estado de la conexión.
- RestartInProgress, usado por el GW para notificar que un grupo de conexiones se encuentran en falla o reinicio.
- EndpointConfiguration, usado para indicar al GW las características de codificación esperadas en el extremo final.

Con ambos extremos conectados, se entrega la señal de llamada al extremo del GW-B y finalmente se establece la conexión entre extremos.

2.4 INDICADORES DE ANÁLISIS EN UNA RED VOZ SOBRE IP

En esta sección se trata de explicar algunos de los problemas a los que se enfrenta una red VoIP y la manera en la que pueden afectar a las redes paquetizadas.

2.4.1 LATENCIA

El retardo o latencia en VoIP se caracteriza por el tiempo en el que la voz tarda en producirse en el que está hablando y llegar al oído del que está escuchando. El retardo, que está causado por distintas fuentes, es presumiblemente el efecto más notorio y perjudicial para este tipo de redes. En el estándar G.114 de la ITU-T se especifica que el retardo máximo permisible en una comunicación extremo a extremo en una llamada de voz debe de ser de 150ms. De esta manera podemos establecer una cierta distinción de zonas de retardo, como la siguiente:

- 0-150ms: retardo no percibido por el destinatario final
- 150-400ms: retardo perceptible pero aún es aceptable
- 400ms: retardo inaceptable

Las fuentes del retardo son:

- Retardo del Codec (algorítmico y de procesado)
- Retardo de propagación (Propagation delay)
- Retardo de serialización (Serialization delay)

- Retardo introducido por la red (Network delay)

Un ejemplo podría ser la Figura 11 basada una red del tipo G.729A:

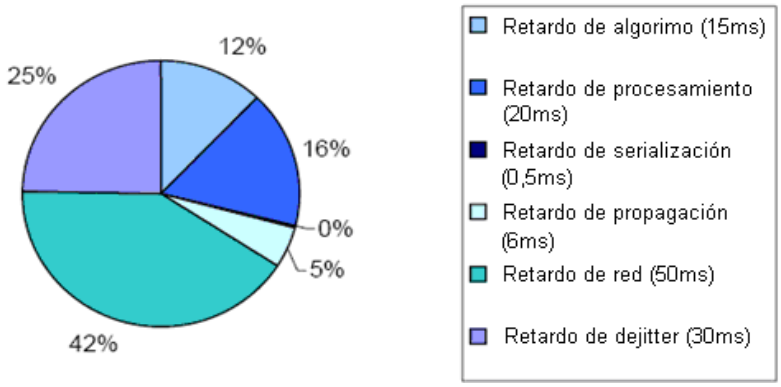

Figura 11. Relevancia de los retardos

El **Retardo por Codec** se halla a partir de una contribución de dos tipos diferentes de retardo, el que introduce el propio codec, denominado retardo algorítmico, y el retardo de procesado, que incluye el tiempo que se tarda en codificar las muestras de voz y empaquetarlas adecuadamente. La Tabla III muestra algunos valores de retardo por CODEC.

Tabla III. Valores de Retardo de CODECS

Codec	Tasa	Tamaño De trama	Retardo optimista	Retardo pesimista
ADPCM, G.726	32 Kbps	10ms	2.5ms	10ms
CS-ACELP,G.729A	8 Kbps	10ms	2.5ms	10ms
MP-MLQ, G.723.1	6.3 Kbps	30ms	5ms	20ms
MP-ACELP, G.723.1	5.3 Kbps	30ms	5ms	20ms

El **Retardo de propagación** es el tiempo que tardan los paquetes en circular o viajar por el medio físico de transporte de un extremo a extremo. Por lo tanto, su valor dependerá directamente del medio físico que se esté empleando.

El **Retardo de serialización** se basa en el tiempo que se requiere para pasar un paquete de un buffer a un enlace o viceversa. Este tipo de retardo presentará valores diferentes en función tanto del tamaño del paquete como por la velocidad del enlace que se use. La Tabla IV muestra algunos retardos de serialización:

Tabla IV. Valores de retardo de serialización

Tamaño de la trama							
Velocidad Del enlace	**1 byte**	**64 bytes**	**128 bytes**	**256 bytes**	**512 bytes**	**1024 bytes**	**1500 bytes**
56 Kbps	143 µs	9 ms	18 ms	36 ms	72 ms	144 ms	214 ms
64 Kbps	125 µs	8 ms	16 ms	32 ms	64 ms	128 ms	187 ms
128 Kbps	62.5 µs	4 ms	6 ms	16 ms	32 ms	64 ms	93 ms
256 Kbps	31 µs	2 ms	4 ms	8 ms	16 ms	32 ms	48 ms
512 Kbps	15.5 µs	1 ms	2 ms	4 ms	8 ms	16 ms	23 ms
768 Kbps	10 µs	840 µs	1.28 ms	2.56 ms	5.12 ms	10.24 ms	15 ms
1536 Kbps	5 µs	220 µs	840 µs	1.28 ms	2.56 ms	5.12 ms	7.5 ms

El **Retardo introducido por la red** es uno de los eventos que participan en la congestión de la red. Por ello, es uno de los retardos más significativos por su gran relevancia.

No hay una solución que se pueda implementar de manera sencilla. Muchas veces depende de los equipos por los que pasan los paquetes, es decir, de la

red misma. Se puede intentar reservar un ancho de banda de origen a destino o señalizar los paquetes con valores de ToS para intentar que los equipos sepan que se trata de tráfico en tiempo real y lo traten con mayor prioridad pero actualmente no suelen ser medidas muy eficaces ya que disponemos del control de la red.

2.4.2 JITTER

El Jitter es el tiempo variable entre llegadas de paquetes causado por la red, es otro de los problemas de retardo a analizar en temas de calidad de servicio. Con ese motivo se hace evidente que los paquetes deberán ser almacenados y retenidos lo suficiente como para ordenarlos y reproducirlos en su secuencia correcta. Por lo tanto, este proceso conlleva un retardo adicional y preciso de un diseño o adaptación del tamaño del buffer de “de-jitter”.

Para poder adaptar el tamaño del buffer existen dos soluciones diferentes, escogiendo la mejor en función del tipo de red de paquetes que se use:

- La primera solución consiste en medir cuanto varia el nivel de los diferentes paquetes en un corto periodo de tiempo en el buffer de “de-jitter” y de forma gradual iremos adaptándolo hasta llegar al jitter óptimo. Esta versión es óptima sobre todo para redes que presentan un jitter poco variable o consistente.
- En cambio la segunda solución se basa en contar los paquetes que lleguen tarde y crear así una relación entre estos paquetes y el número de paquetes

que sí se han procesado correctamente. Dicha relación es la que se usará para poder ajustar el tamaño del buffer correctamente en función de la relación de paquetes tardíos permitida. Esta versión es mejor para redes con alta variabilidad de jitter, es decir, para redes IP.

2.4.3 ECO

En las redes de telefonía el eco es causado por las reflexiones generadas por el circuito híbrido que convierte el circuito de 4 hilos (un par para transmisión y otro par para recepción) a 2 hilos, el típico par de cobre que todo cliente tiene para recibir y transmitir. Esto conduce a que un propio interlocutor puede escuchar su propia voz. La Figura 12 ilustra el efecto del eco.

Figura 12. Eco causado por reflexiones en el circuito

Los canceladores de eco, cuyo estándar es el G.165 de la ITU-T, deben cumplir unos requisitos muy estrictos comparando los datos de voz recibidos por la red de paquetes con los datos de voz enviados, además también se debe eliminar la participación del circuito híbrido con un filtro digital.

2.4.4 EFICIENCIA

La eficiencia, relacionada a la pérdida de paquetes, es la tasa o porcentaje de paquetes recibidos correctamente. Para una mayor exactitud del registro de pérdida de paquetes, se deben tener en cuenta tanto los paquetes que se pierden como los que se reciben erróneamente y los paquetes que se descarten al retrasarse más de lo permisible.

La pérdida de paquetes, cuyo origen está en la congestión propia de la red, depende de la capacidad de los búffers y de los retrasos de los paquetes. Su efecto varía, ya que podemos pasar de una total transparencia de cara al usuario, a considerarse intolerable con la presencia de ráfagas de errores, que perjudican aún más la tasa de error que los simples errores intermitentes o más distribuidos. De hecho existen los siguientes intervalos:

- Menos del 5% → no detectable por el usuario
- Entre el 5% y el 10% → puede ser tolerable en función de la estrategia de reemplazo de paquetes (loss concealment)
- Más del 10% → intolerable

2.4.5 MODULACIÓN PCM

Se denomina modulación al proceso de colocar la información contenida en una señal, generalmente de baja frecuencia, sobre una señal de alta frecuencia.

La fuente de información puede presentarse de varias maneras. Puede estar ya en formato digital, con lo cual puede saltarse el proceso de formateo. Puede ser información tipo texto, con lo cual la conversión a dígitos binarios se hace usando un código de conversión. O bien la información puede presentarse en forma analógica, con lo cual el formateo se realiza en tres pasos: **muestreo, cuantización y codificación**. En todos los casos siempre resulta una secuencia de dígitos binarios. Según el teorema de Nyquist una señal debe ser muestreada por lo menos el doble del rango de frecuencia. Los humanos podemos oír frecuencias de hasta 20 KHz, pero la mayoría de la información que se transmite en una conversación no excede de los 4 KHz. En un teléfono analógico, las señales se filtran antes del muestreo para que la mayor parte de la señal se encuentre entre los 300 y 3400 Hz. La misma señal es muestreada a 8000 Hz para que las frecuencias de hasta 4000 Hz puedan también registrarse. Con un muestreo de 8000Hz, cada 125 microsegundos (1/8000), el valor de la señal del teléfono analógico es transmitida a la función cuantizadora.

La cuantización es el proceso de redondear los valores muestreados al valor discreto predefinido más próximo. Debe considerar dos variables muy importantes.

- Número de niveles de cuantización
- Distribución de los niveles de cuantización

Como consecuencia del muestreo tenemos un conjunto de impulsos modulados en amplitud espaciados por intervalos regulares de tiempo, caracterizados

porque sus amplitudes varían de forma analógica, pudiendo adoptar cualquier valor. En la etapa de cuantificación se hacen corresponder estos valores con un número finito previamente determinado, definiendo por tanto una escala de valores fijos y asignando a ellos las amplitudes comprendidas entre dos ciertos valores consecutivos.

La recomendación G.711 del UIT-T describe la MODULACIÓN POR IMPULSOS CODIFICADOS (MIC) DE FRECUENCIAS VOCALES. Existen dos formas de cuantización distintas:

- **Cuantización PCM uniforme**

  Como se muestra en la Figura 13, se toman valores equidistribuidos en el eje positivo (normalmente 127) y otros 127 en el negativo. Así, para cada muestra necesitaremos 127*2+1=255 posibles valores, de forma que se necesitan 8 bits/muestra para lograr la codificación.

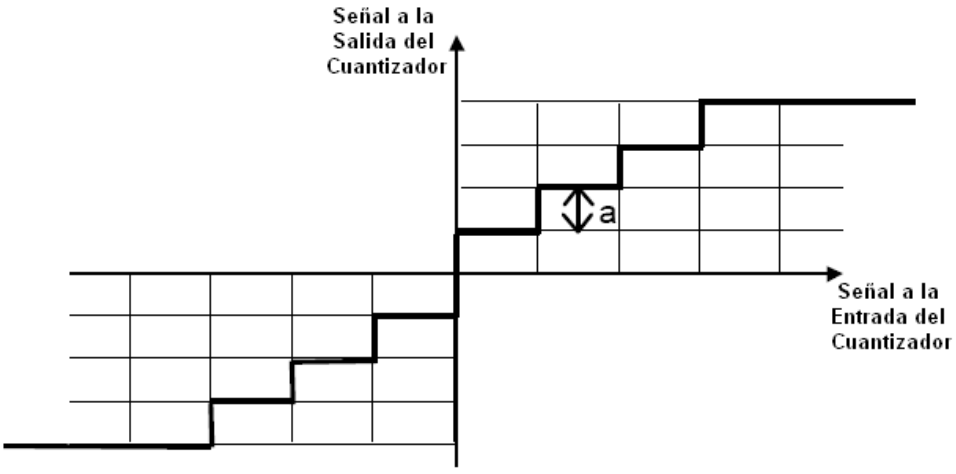

Figura 13. Cuantización uniforme

- **Cuantización no uniforme**

  En este caso los intervalos de cuantización se distribuyen de manera no uniforme. El tamaño de los intervalos de cuantización se determina en función de la SNR y la señal de menor potencia que se va a codificar, de forma que la SNR permanezca constante. El tamaño del escalón será más reducido en los valores pequeños de la señal que en los grandes. Existen dos tipos de cuantización no uniforme en PCM. La cuantización con ley A, utilizada en los países Europeos y la cuantización con ley μ utilizada en Japón y EEUU. La norma G.711 especifica que los trayectos digitales entre países que hayan adoptado leyes de codificación diferentes deberán efectuar la transmisión con señales codificadas según la ley A. Cuando los dos países hayan adoptado la misma ley, deberá utilizarse esa ley en los trayectos digitales entre los mismos. Incumbirá a los países que utilicen la ley μ efectuar toda conversión necesaria.

  Como indica la Figura 14 la ley A linealizada tiene 13 segmentos (la ley μ tiene 15). Las características son simétricas respecto del origen, por eso las figuras sólo representan la mitad positiva. Los dos segmentos de las mitades positiva y negativa que coinciden en cero tienen la misma pendiente, por lo que se puede considerar como un solo segmento. Los valores más utilizados son A=87.3 y μ=255.

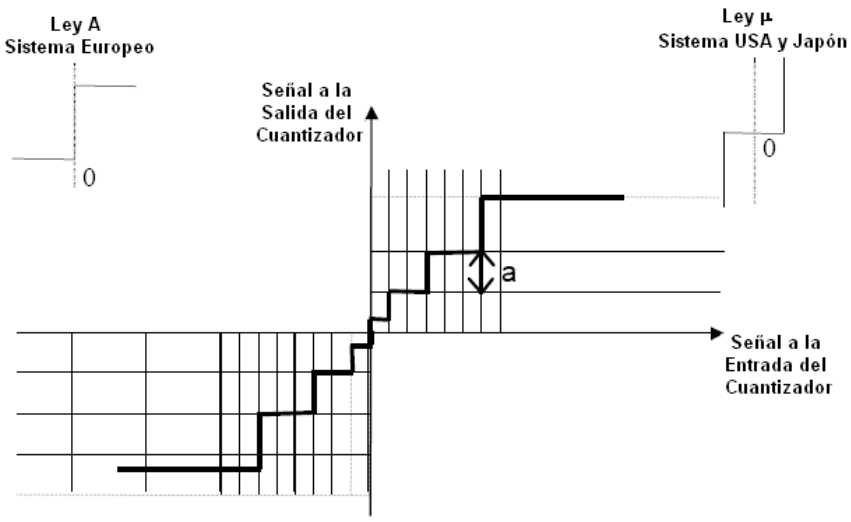

Figura 14. Cuantización no uniforme

La **Codificación** es el proceso que consiste en convertir los pulsos cuantificados en un grupo equivalente de pulsos binarios de amplitud constante. Este es el último de los procesos que tiene lugar durante la conversión analógica-digital

A cada valor anteriormente determinado en el proceso de cuantización se le hace corresponder un conjunto de bits, impulsos de amplitud fija (unos) o ausencia de impulsos (ceros).

2.4.6 COMPRESIÓN DE VOZ

Como explicamos anteriormente se utilizan dos variaciones básicas de PCM de 64 Kbps: la ley μ y la ley A. Sin embargo, existe otro método de compresión que es la ADPCM (modulación de código de pulso diferencial adaptivo). Un

ejemplo de ADPCM es la ITU-T G.726, que codifica utilizando muestras de 4 bits, lo que resulta en una velocidad de transmisión de 32 Kbps. A diferencia de la PCM, los 4 bits no codifican directamente la amplitud de la voz, sino que codifican las diferencias de la amplitud, y la velocidad de cambio de esa amplitud. PCM y ADPCM son técnicas de codificación por forma de ondas, que se basan en explotar las técnicas redundantes de la forma de ondas.

El proceso de convertir ondas analógicas a información digital se hace con un codificador-decodificador (el CODEC). Hay muchas maneras de transformar una señal de voz analógica, todas ellas gobernadas por varios estándares. El proceso de la conversión es complejo. Además de la ejecución de la conversión de analógico a digital, el CODEC comprime la secuencia de datos, y proporciona la cancelación del eco. La compresión de la forma de onda representada puede permitir el ahorro del ancho de banda. Otra manera de ahorrar ancho de banda es el uso de la supresión del silencio.

2.4.6.1 NORMAS DE CODIFICACIÓN DE VOZ

La ITU-T normaliza los esquemas de codificación CELP, MP-MLQ PCM y ADPCM en sus recomendaciones de la serie G. Entre los estándares más utilizados para telefonía y VoIP se mencionan en la Tabla V:

Tabla V. Estándares de codificación de voz

Nombre	Stándar	Descripción	Bit rate (kb/s)	Sampling rate (kHz)	Frame size (ms)	Observaciones	MOS (Mean Opinion Score)
G.711	ITU-T	Pulse code modulation (PCM)	64	8	Muestreada	Dos versiones U-law y A-law	4.1
G.722	ITU-T	7 kHz audio-coding dentro de 64 Kbps	64	16	Muestreada	Divide los 16 Khz en dos bandas cada una usando ADPCM	
G.722.1	ITU-T	Codificación a 24 y 32 Kbps para sistemas sin manos con baja pérdida de paquetes	24/32	16	20		
G.723	ITU-T	Extensión de la norma G.721 a 24 y 40 Kbps para aplicaciones en circuitos digitales.	24/40	8	Muestreada	Obsoleta por G.726. Es totalmente diferente de G.723.1.	
G.723.1	ITU-T	Codificador de doble velocidad para comunicaciones multimedia que transmite en 5.3 y 6.3 Kbps	5.6/6.3	8	30	Parte de H.324 video conferencing. Codifica la señal usando análisis predictivo lineal Para el codificador de alta velocidad utiliza Multipulse Maximum Likelihood Quantization (MP-MLQ) y para el de baja velocidad, Algebraic-Code-Excited Linear-Prediction (ACELP).	3.8-3.9
G.726	ITU-T	40, 32, 24, 16 Kbps adaptive differential pulse code modulation (ADPCM)	16/24/32/40	8	Muestreada	ADPCM; reemplaza a G.721 y G.723.	3.85
G.727	ITU-T	5-, 4-, 3- and 2-bit/muestra con adaptive differential pulse code modulation (ADPCM)	varía		Muestreada	ADPCM. Relacionada con G.726.	
G.728	ITU-T	Codificación de 16 Kbps usando codigó de bajo retardo (Linear Prediction)	16	8	2.5	CELP.	3.61
G.729	ITU-T	Codificación de 8 Kbps usando (CS-ACELP)	8	8	10	Bajo retardo (15 ms)	3.92

2.4.7 PROTOCOLOS DE TRANSPORTE

En IP se desplazan dos tipos de tráfico: UDP (Protocolo de Datagrama de Usuario) y TCP. En general se utiliza TCP cuando se necesita una conexión fiable y UDP cuando se necesita simplicidad. Considerando que el transporte de voz es sensible al tiempo del tráfico de voz se elige UDP/IP para ello, pues se

necesitaba más información en una base paquete a paquete que la que ofrecía UDP. Por lo tanto, para el tráfico en tiempo real o sensible al tráfico, el IETF adoptó el RTP. VoIP circula en la parte superior del RTP, que circula a su vez en la parte superior del UDP. Por lo tanto, VoIP es transportado con una cabecera de paquete RTP/UDP/IP.

2.4.7.1 Protocolo de Transporte de Tiempo Real RTP

El RTP es el protocolo para transmitir tráfico sensible al retraso por redes paquetizadas. RTP da a las estaciones receptoras información que no está en las corrientes UDP/IP sin conexión. En la Figura 14 se muestra la cabecera de RTP. Se observa que hay dos bits de información importantes: la secuencia y la marca de temporización.

Versión	IHL	Tipo de servicio	Longitud total	
Identificación			Indicaciones	Compensación de fragmentos
Tiempo de existencia		Protocolo	Suma de verificación de cabecera	
Dirección de origen				
Dirección de destino				
Opciones			Relleno	

Puerto de origen	Puerto de destino
Longitud	Suma de verificación

V=2	P	X	CC	M	PT	Número de secuencia
Marca para la temporización						
Identificador de origen de sincronización (SSRO)						

Figura 15. Cabecera RTP

RTP utiliza información de secuencia para determinar si los paquetes están llegando en orden y la marca de temporización se utiliza para determinar el tiempo de llegada entre paquetes. RTP consta de una parte de datos y una parte de control, que es llamada RTCP

(Protocolo de control de Tiempo Real). RTCP trabaja con RTP para realizar estadísticas del tráfico, como por ejemplo el número de bytes enviados, los paquetes enviados y perdidos, el jitter o desorden de llegada, o el tiempo de latencia.

Se puede comprimir la cabecera RTP a 2 o 3 bytes utilizando Compresión de Cabecera RTP.

2.4.7.2 Protocolo de Datagrama de Usuario UDP

Es un protocolo del nivel de transporte basado en el intercambio de datagramas. Permite el envío de datagramas a través de la red sin que se haya establecido previamente una conexión, ya que el propio datagrama incorpora suficiente información de direccionamiento en su cabecera; pero no tiene confirmación ni control de flujo. Su uso principal es para protocolos como DHCP, BOOTP, DNS y demás protocolos en los que el intercambio de paquetes de la conexión/desconexión son mayores, o no son rentables con respecto a la información transmitida, así como para la transmisión de audio y vídeo en tiempo real, donde no es posible realizar retransmisiones por los estrictos requisitos de retardo que se tiene en estos casos. En la familia de protocolos de Internet UDP proporciona una sencilla interfaz entre la capa de red y la capa de aplicación. UDP no otorga garantías para la entrega de sus mensajes y el origen UDP no retiene

estados de los mensajes UDP que han sido enviados a la red. UDP sólo añade multiplexado de aplicación y suma de verificación de la cabecera y de la información útil. Cualquier tipo de garantías para la transmisión de la información, deben ser implementadas en capas superiores. La Figura 16 muestra la estructura UDP.

+	Bits 0 - 15	16 - 31
0	Puerto origen	Puerto destino
32	Length	Verificación de suma
64	Datos	

Figura 16. Estructura de UDP

La cabecera UDP consta de 4 campos de los cuales 2 son opcionales, las mismas que se muestran con fondo rojo en la Figura 16. A los campos del puerto origen le sigue un campo obligatorio que indica el tamaño en bytes del datagrama UDP incluidos los datos. El valor mínimo es de 8 bytes. El campo de la cabecera restante es un checksum de 16 bit que abarca la cabecera y los datos. El checksum también es opcional, aunque generalmente se utiliza en la práctica.

2.5 PRINCIPALES VENTAJAS DE VOZ SOBRE IP

Para hablar de todas las ventajas existentes de poseer una Red Telefónica basada en IP en las Fuerzas Armadas del Ecuador, primero debemos señalar que la utilización de las tecnologías basadas en el protocolo IP se ha convertido en un

elemento estratégico del diseño, realización y utilización de las redes de telecomunicaciones. Es por ello que los miembros del Comando Conjunto o COMACO (máximo organismo de planificación, preparación y conducción estratégica de las operaciones militares y de asesoramiento sobre las políticas militares) muestran un interés cada vez mayor en las diferentes prestaciones que brinda esta técnica.

Por lo anteriormente expuesto nos permitimos señalar las siguientes ventajas:

I. Una de las razones claves para combinar las redes de voz y datos es el ahorro económico en el servicio que se brinda. A pesar de que la Red MODE (nombre de la actual red telefónica) del Comando Conjunto no está concebida con fines de lucro, podemos decir que el costo del servicio no depende de la ubicación física de la red - como ocurre con redes fijas de fibra óptica o par de cobre - y no es tan sensible a la dispersión de las unidades militares o la ubicación de cada uno de los usuarios.

II. En una red militar, la convergencia de las redes de voz y datos permite poseer menos circuitos en la PSTN. De la misma manera, una infraestructura de IP (que utilice teléfonos IP) requiere menos añadidos, desplazamientos y cambios que una red tradicional de voz y datos. Esto se debe a que con esta infraestructura se pueden utilizar funciones de datos como el DHCP, es decir la dirección IP no necesita estar configurada estáticamente en el dispositivo. Por tanto si se tiene un teléfono IP configurado con DHCP, se puede llevar a cualquier lugar en el que sea necesario y seguirá manteniendo el mismo número de teléfono (mover un teléfono conlleva costes laborales y de reconfiguración de la Central de Conmutación). Esto es parecido a trasladar la

computadora portátil de una oficina a otra y seguir pudiendo entrar en el mismo servidor de red.

III. Una tecnología cuyo empleo se masifica cada día es WiFi y WiMax, mismas que de emplearse brindarían movilidad en un radio de cobertura determinado, y con un ancho de banda aceptable en ese radio sería indiferente la densidad de población militar o unidades militares existentes (aunque a mayor distancia de la antena base menor es el rendimiento). Las nuevas tecnologías mencionadas amplían el radio de servicio local, la tecnología WiFi permite un rendimiento de 5 Mbps sobre un radio de unos 100 metros, extensible a 10 Km con una antena de línea visual unidireccional, que permite a un pequeño operador prestar un servicio a toda una comarca conectándose por un vínculo a la red IP fija; la versión avanzada de WiFi, WiMax, permitirá un rendimiento aún mayor, del orden de 1.5 – 2 Mbps en un radio de 3 Km sin línea de vista (en la banda con licencia 2.5 Ghz) y hasta 25-35 km con una antena unidireccional de línea visual. Los nuevos teléfonos móviles que operan sobre IP inalámbricos (VoWiFI), bajarán de precio rápidamente y permitirán prestar un servicio local aún más flexible a las zonas distantes y que requieran cobertura de comunicación militar.

IV. Por su naturaleza, las Fuerzas Militares deben tener coberturas en lugares remotos, donde no se han hecho inversiones en cableado o medios para el transporte de comunicaciones. Sin embargo, el servicio básico requerido es el teléfono, y algunas aplicaciones clave interactivas como correo electrónico y navegación. Al migrar la Red de las Fuerzas Armadas de conmutación de circuitos a VoIP lograríamos integrar a cada una de las unidades militares a los

Centros de Comando de una forma ágil y oportuna, proveyéndoles de servicios de telefonía, Internet, correo, etc. Ello les permite implementar una serie de aplicaciones importantes como son transporte de imágenes (cuadro de situación militar), telefonía criptografiada, etc.

V. La infraestructura se hace mucho más simple en la telefonía paquetizada transportada sobre una Red de datos, ya que en la telefonía convencional se debe tener separadas las redes de voz y datos como se muestra en la Figura 17 dificultando el control de las mismas, mientras que en una red moderna van a coexistir ambas redes, en un mismo medio como se muestra en la Figura 18.

VI. Otra ventaja de VoIP es la posibilidad de tener un departamento de Servicios de Información (IS) que soporte ambas redes de voz y datos (ya que las redes son ahora una entidad). Al principio esto puede provocar tensiones entre esas dos infraestructuras, pero al igual que ocurre con cualquier revolución tecnológica mediante la técnica de prueba y error se subsanarán estas vicisitudes.

VII. Al migrar a VoIP, las herramientas de infraestructura habituales ya no se necesitarán por mucho tiempo. Entre ellas se encuentran herramientas como los puertos físicos para servicios como el correo de voz. En una red de conmutación de circuitos, el correo de voz se vende sobre la base del número de buzones de correo y el número de puertos físicos que se necesitan para soportar usuarios simultáneos. Con VoIP, ya no son necesarios los puertos físicos de circuitos conmutados. El servidor de correo de voz solo necesita tener una conexión IP (Ethernet, ATM, PDH, SDH, etc).

VIII. VoIP también permite que los sistemas de correo de voz se coloquen en plataformas que empleen diferentes estándares (como PC, máquinas UNIX).

Cuando una función (correo de voz) está en una plataforma basada en estándares, es poco probable que el precio sea desorbitado. Por ejemplo el costo de un megabyte de espacio de disco duro para un proveedor de Correo de voz en una PSTN es 20 veces mayor que el precio medio por megabyte de los discos duros empleados en una Red de VoIP.

IX. La escalabilidad es otro de los factores dirimentes al escoger el tipo de telefonía a emplear, en este caso una red que converge sus servicios brinda mayores ventajas al momento de hacer crecer la red, ya que lo único que hay que hacer es extender mi red de datos y contratar mayor ancho de banda para el transporte en la capa física.

Es necesario dejar claro que el deseo a futuro de las Fuerzas Armadas es combinar redes de distinta índole, voz y datos, que permitan el desarrollo de nuevos conceptos y tecnologías, como lo es la voz paquetizada.

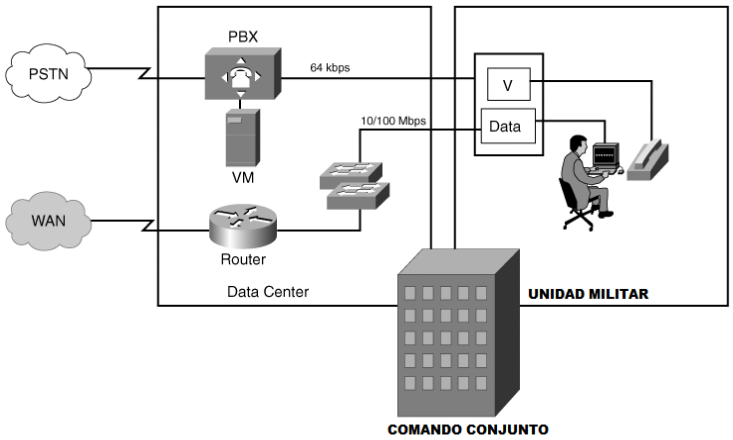

Figura 17. Redes de Voz y Datos separadas

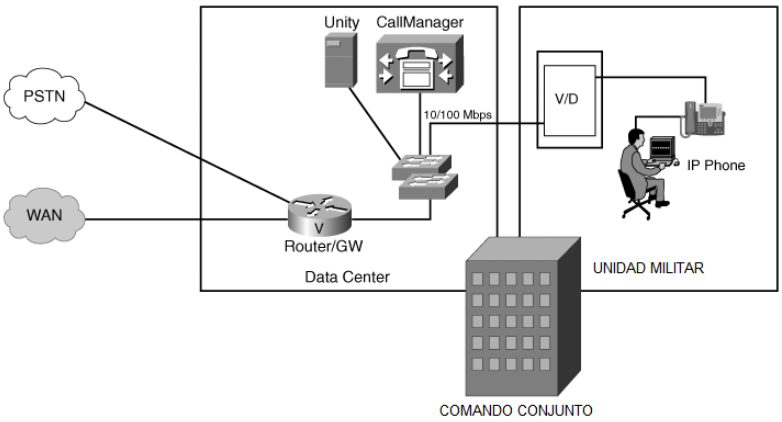

Figura 18. Red de Nueva Generación

3. METODOLOGÍA PARA EL DESARROLLO DE SOLUCIONES EN TELEFONÍA IP

3.1 INTRODUCCIÓN A LA METODOLOGÍA PDIOO

Para el desarrollo de una red de Telefonía IP (IPT), es necesario el seguimiento de una Metodología que cubra las fases de Planificación, Diseño, Implementación, Operación y Optimización (PDIOO). Esta metodología garantiza escalabilidad y mejora de la eficiencia de las redes. Este trabajo se enfocará únicamente en el desarrollo de las fases de Planificación y Diseño de la red de IPT de las Fuerzas Armadas, por tal motivo no se mencionarán o analizarán los costos que implicaría la implementación del diseño propuesto.

Los ingenieros diseñadores de redes debemos tener conceptos sólidos de tecnología de voz paquetizada, equipos de voz, interacción de redes TDM, tecnología IP y sus componentes y por lo tanto, debemos estar comprometidos con la Metodología PDIOO de redes IP.

La Figura 19 mostrará las tareas inherentes a la Metodología PDIOO para el desarrollo de soluciones de IPT.

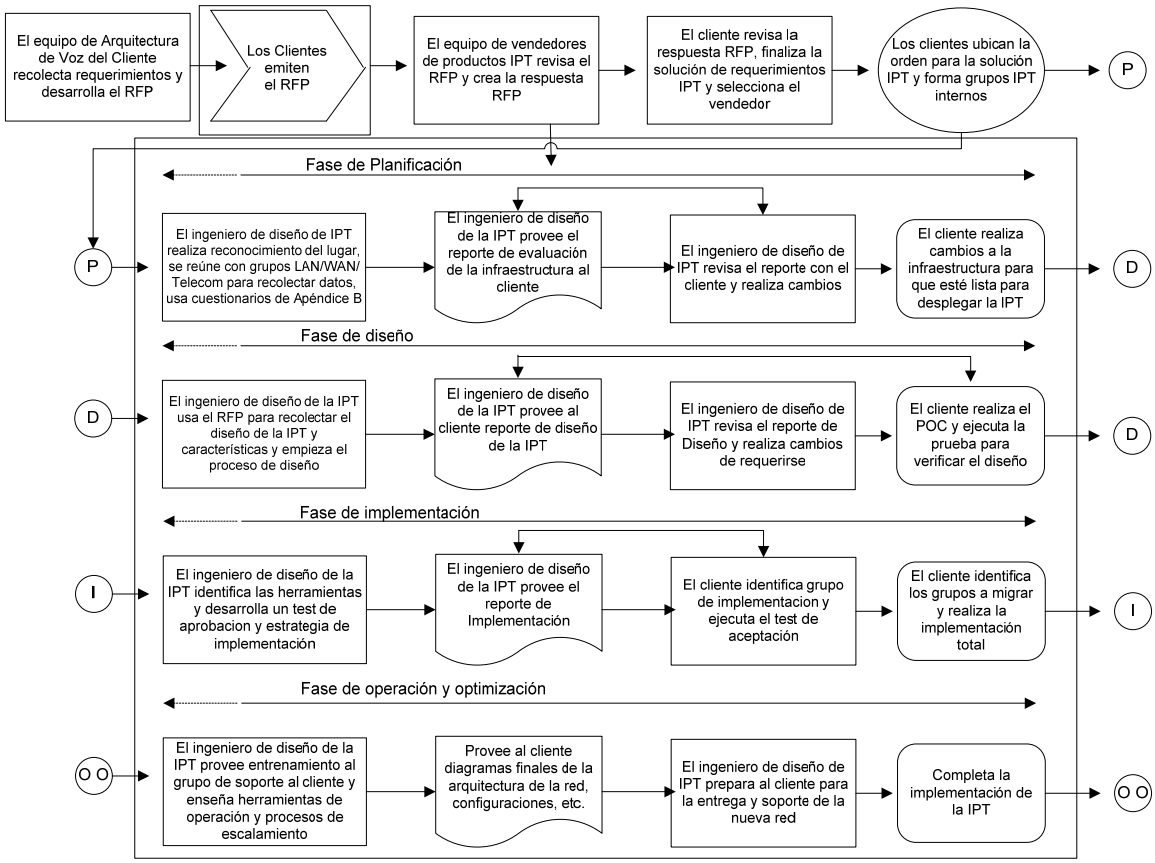

Figura 19. Metodología para implementación de soluciones IPT

3.2 FASE DE PLANIFICACIÓN

Es la primera fase de la metodología PDIOO. Una de las tareas más importantes de esta fase es conocer los requerimientos y expectativas de la empresa (en este caso la Red de Comunicaciones de las Fuerzas Armadas); para ello se deben considerar dos categorías:

- Expectativas y requerimientos operacionales
- Expectativas y requerimientos técnicos

Desde el punto de vista de las expectativas y requerimientos operacionales, deben considerarse los objetivos y la visión de las Fuerzas Armadas del Ecuador y analizar su relación con futuras redes de IPT. Este punto que abarca específicamente información que servirá de ayuda para ejecutar el proyecto de una forma oportuna y completarla como se proyecta, incluye también los objetivos de la empresa en cuanto a expansión de su red en los próximos 3 a 5 años, y sus expectativas respecto al tiempo que tomará el proyecto en planificarse, diseñarse e implementarse.

Con respecto a las expectativas y requerimientos técnicos, deben considerarse las futuras necesidades de las Fuerzas Armadas con relación a las características y funcionalidades de la red de IPT.

Luego de conocer las expectativas y requerimientos de alto nivel, el siguiente paso será realizar un reconocimiento del lugar. En esta fase, deberemos obtener los siguientes detalles:

- Infraestructura de LAN existente (topología, equipos y políticas de Calidad de Servicio QoS(Quality of Service))
- Infraestructura de WAN (arquitectura, equipos, políticas de QoS, flujos de tráfico, asignación de ancho de banda y empleo del enlace existente)
- Infraestructura de capa 3 y capa 2
- Esquema de direccionamiento IP (despliegue de servicios DHCP y DNS)
- Enrutamiento de capa 3 y protocolos enrutados utilizados en la red
- Infraestructura de la telefonía tradicional y sus características
- Configuraciones de los planes de discado
- Utilización y desempeño de las Redes de voz y datos
- Infraestructura de manejo de la red existente.

Luego de la recolección de la información descrita anteriormente, desarrollaremos una evaluación de la infraestructura de la red para asegurar de que soportará la IPT, y que serán compatible los nuevos sistemas y aplicaciones con el sistema y dispositivos existentes, y que la IPT se desarrollará de la forma planificada.

La correcta ejecución de la fase de planificación se llevará de la siguiente manera:

- Expectativas objetivas de escalabilidad, desempeño y características del nuevo sistema de IPT
- Infraestructura de una red capaz de soportar tráfico de IPT
- Identificación de recursos apropiados para acelerar el desarrollo de la IPT
- Una red de IPT alineada con necesidades operacionales o requerimientos de alto nivel

- Implementación de aplicaciones de IPT y su integración con aplicaciones existentes

3.3 FASE DE DISEÑO

Después de completar la fase de planificación, deberemos empezar a trabajar en la fase de diseño de la red IPT. El objetivo de esta fase es plantear un diseño de red utilizando la información recolectada de la fase de planificación y la información que especifica las características de requerimientos de la IPT.

Deberemos considerar muchos factores antes de llegar a un diseño final. Esta propuesta de diseño deberá atender a las futuras necesidades de las Fuerzas Armadas del Ecuador.

La fase de diseño consiste en los siguientes requerimientos de Alto Nivel, que coadyuvarán al diseño de las diferentes áreas críticas de la red:

- Diseño de la infraestructura de la red
- Diseño de la infraestructura del proceso de llamada y sus aplicaciones

Como se mostró en la Figura 19, el objetivo de la fase de diseño es completar las cuatro tareas precedentes de la fase de diseño y proveer el documento de diseño que propone un diseño de red que satisface las necesidades de las Fuerzas Armadas del Ecuador.

Como diseñadores de la red de IPT, revisaremos este documento de diseño con el equipo encargado de la administración de la red de las Fuerzas Armadas del Ecuador para asegurarnos de que lo propuesto obedece a sus requerimientos.

3.3.1 DISEÑO DE LA INFRAESTRUCTURA DE RED

La primera tarea de la fase de diseño es habilitar la infraestructura de la red existente en las Fuerzas Armadas para que soporte la red de IPT. Debemos enfocarnos en las siguientes áreas:

- Elección de un modelo de implementación de IPT
- Diseño de un esquema de direccionamiento IP, VLANs de voz para dispositivos de redes de IPT y enrutamiento IP
- Evaluación y selección de modelos de teléfono
- Diseño de servicios DHCP y TFTP para los teléfonos IP y otras terminales de la IPT como adición al uso de servicios DNS.
- Diseño de QoS en la LAN de las Fuerzas Armadas
- Diseño de la infraestructura de LAN y WAN para su flexibilidad
- Dimensionamiento de enlaces WAN y diseño de QoS en la WAN de las Fuerzas Armadas

3.3.2 DISEÑO DE LA INFRAESTRUCTURA DE PROCESO DE LLAMADA Y APLICACIONES

La segunda tarea de la fase de diseño será elegir y dimensionar los componentes de la IPT, revisar y hacer recomendaciones para integrar en la red

de las Fuerzas Armadas aplicaciones de telefonía actuales con y hacia nuevas aplicaciones de IPT basadas en los requerimientos del cliente. Estas tareas se definen como:

- Dimensionar los clusters de CallManager
- Dimensionar los gateways de voz y gatekeeper
- Preparar el sistema de IPT para integrar o acceder al LDAP (Lightweight Directory Access Protocol, servicio de directorio para acceder a depósitos de información referente a usuarios, contraseñas y otras entidades en un entorno de red)
- Diseño del plan de discado
- Incorporar requerimientos de fax y MODEM en la red de IPT
- Recomendar soluciones de seguridad y de administración de red

3.4 FASE DE IMPLEMENTACIÓN

Luego de haber documentado la fase de diseño, la siguiente fase es la implementación. Esta fase permite asegurar que la red desarrollada tendrá todas las funcionalidades deseadas. Involucra el desarrollo de la estrategia y procedimientos de implementación.

En redes grandes, como lo constituye la red de las Fuerzas Armadas, se deberá subcontratar algunas de las tareas de implementación, como la implementación de los teléfonos IP, la configuración de los teléfonos IP en el CallManager, etc. Por lo

tanto, definir el proceso es importante para que los subcontratistas puedan llevar este proceso y sigan la metodología desarrollada. Esto asegurará la oportuna resolución de problemas que puedan ser encontrados durante la implementación.

Una buena estrategia para la implementación de IPT en redes grandes es dividir el proyecto en fases pequeñas. También se deberán monitorear las estadísticas de utilización de la red de las Fuerzas Armadas y la funcionalidad de la nueva red desplegada en cada etapa. Mantener un registro de los problemas reportados por el usuario y modificar los procesos de implementación para asegurar que los usuarios de la red de IPT no encuentren los mismos problemas. Los problemas presentados deben ser solucionados antes de implementaciones adicionales.

Una estrategia de implementación de la red de IPT debería tener mínimo los siguientes pasos claramente definidos y documentados:

- Identificar el equipo de implementación, conformado por miembros de la administración de la red, responsables para proveer el nuevo sistema de IPT a la red de producción
- Identificar y estandarizar las herramientas de implementación que son útiles en el despliegue de teléfonos IP y de otros terminales de IPT
- Documentar los pasos de instalación y configuración para varios dispositivos
- Definir los grupos de usuario en donde se realizará la implementación y el tiempo de empleo para ello
- Informar a los usuarios de la red de las Fuerzas Armadas sobre el sistema telefónico entrante y entrenarlos en las características de los nuevos teléfonos

- Preparar un sistema de administración de números telefónicos para seguir las asignaciones de números de teléfonos
- Garantizar que exista una comunicación constante entre el equipo de implementación y el personal de diseño para definir los problemas enfrentados y plantear las soluciones respectivas
- Definir los procedimientos de escalamiento para dirigir las características y problemas de funcionalidad o requerimientos descubiertos en la implementación
- Proveer al equipo de la red de las Fuerzas Armadas una revisión técnica para alertas relacionadas a las redes de IPT que podrían afectar la implementación de su red de IPT
- Comunicar al equipo ejecutivo de la red y a los usuarios si no hay disponibilidad del servicio, que pudiera ser causado por este despliegue

3.5 FASE DE OPERACIÓN Y OPTIMIZACIÓN

La última fase del ciclo PDIOO es la operación y la optimización. La planificación de la operación protege la inversión de la red y provee al equipo de operación de la red de las Fuerzas Armadas la capacidad de monitorear proactivamente la red para reducir problemas. Los siguientes pasos son importantes para que las Fuerzas Armadas puedan ejecutar una operación exitosa de la red de IPT:

- Proveer entrenamiento y técnica de operación práctica al equipo de soporte en las herramientas operacionales de los productos de IPT y herramientas de administración de red

- Involucrar al equipo de operaciones de la red de las Fuerzas Armadas en la etapa de planificación y la implementación del proyecto IPT
- Definir procedimientos de escalamiento y proveer recursos como las herramientas y productos requeridos; así como contactos con el proveedor de los equipos para las soluciones de problemas reportados por los usuarios
- Definir un proceso para realizar mejoras de hardware y software
- Definir procedimientos para administrar las peticiones de cambio de configuración
- Establecer un contrato de servicio y soporte con el proveedor o proveedores de los equipos de IPT

La fase de optimización involucra ejecutar pasos que ayudan a la red a llevar el mejor desempeño posible, y así disminuir los problemas de la red y posibles interrupciones. Para optimizar la red, el equipo de soporte deberá tener un sólido conocimiento de las herramientas de operación, monitoreo y optimización disponible. Estas herramientas y procesos simplifican la expansión de la red, aseguran la calidad de la red y sus aplicaciones y facilita la solución de problemas.

La metodología PDIOO mencionada permite asegurar un despliegue exitoso de convergencia de la red de datos de las Fuerzas Armadas. El seguimiento de esta metodología garantizará un desarrollo más fácil y eficiente. Las tecnologías que no se desarrollaran siguiendo estos pasos podrían terminar en redes no escalables y poco óptimas.

El desarrollo de este trabajo tratará las fases de planificación y de diseño de la red de IPT de las Fuerzas Armadas. Con ello se dejará listo para la implementación de los nuevos equipos en la red de datos, para realizar su posterior desarrollo junto al equipo responsable de la red de datos en estudio.

4. DOCUMENTO SOLICITUD DE PROPUESTA ENTREGADO POR LAS FUERZAS ARMADAS

Un RFP (Request for Proposal, o solicitud de propuesta) es una herramienta estándar utilizado por gobiernos y empresas para solicitar propuestas de posibles proveedores de productos o servicios, promoviendo así propuestas competitivas entre proveedores.

Las RFP son un componente vital en la administración de proyectos exitosos, ya que definen claramente los entregables asociados con el proyecto y define un marco de acción para la ejecución del mismo. Idealmente los RFP estipulan los requisitos de la empresa que está comprando y las condiciones bajo las cuales contrataría.

La RFP que se desarrolla en este capítulo señala los requerimientos para el sistema de comunicaciones de voz en la red de datos de las Fuerzas Armadas, y para ello lo divide en dos partes:

- Perfil del Cliente
- Requerimientos Técnicos del Cliente

Es importante destacar que el RFP es parte del trabajo de investigación que se realizó en esta tesis, en base a los requerimientos y condiciones señaladas por el Ing. Wilson Freire quien está encargado de la operación de la red de comunicaciones del nodo Guayaquil.

4.1 PERFIL DEL CLIENTE Y ARQUITECTURA EXISTENTE

El Comando Conjunto de las Fuerzas Armadas del Ecuador (COMACO) es una institución de carácter estratégico dentro del Ecuador y son los responsables de la administración, operación y control de la red de comunicaciones de las Fuerzas Armadas. Esta institución debe abarcar todas las regiones del país y debido a las nuevas amenazas existentes tanto en la frontera norte como en toda la costa ecuatoriana (narcotráfico) ha crecido su red de comunicaciones rápidamente. Por ello la red de comunicaciones del COMACO debe mantener las comunicaciones confiables y permanentes de las tres Fuerzas militares (Ejército, Marina y Aviación).

El número de usuarios establecidos se distribuye por nodo y se presenta a continuación en la Tabla VI:

Tabla VI. Número de usuarios de cada nodo de la red de datos

Nombre del sitio	Número de usuarios
Quito	2000
Guayaquil	2600
Machala	700
Coca	700

La Figura 20 muestra la arquitectura de la red de voz y datos existente. Estas redes actúan de forma separada y operan independientemente. Los nodos centrales se encuentran en Quito, Guayaquil, Coca y Machala, de los cuales Quito y Guayaquil son los principales y los otros dos actúan de forma remota. El tráfico de datos entre los cuatro nodos se realiza a través de un enlace WAN PDH con un ancho de banda como el que se muestra a continuación en la Tabla VII.

Tabla VII. Enlaces PDH existentes en la Red del COMACO

	Quito	Guayaquil	Coca	Machala
Quito	0	4 E1	2 E1	2 E1
Guayaquil	4 E1	0	2 E1	2 E1
Coca	2 E1	2 E1	0	2 E1
Machala	2 E1	2 E1	2 E1	0

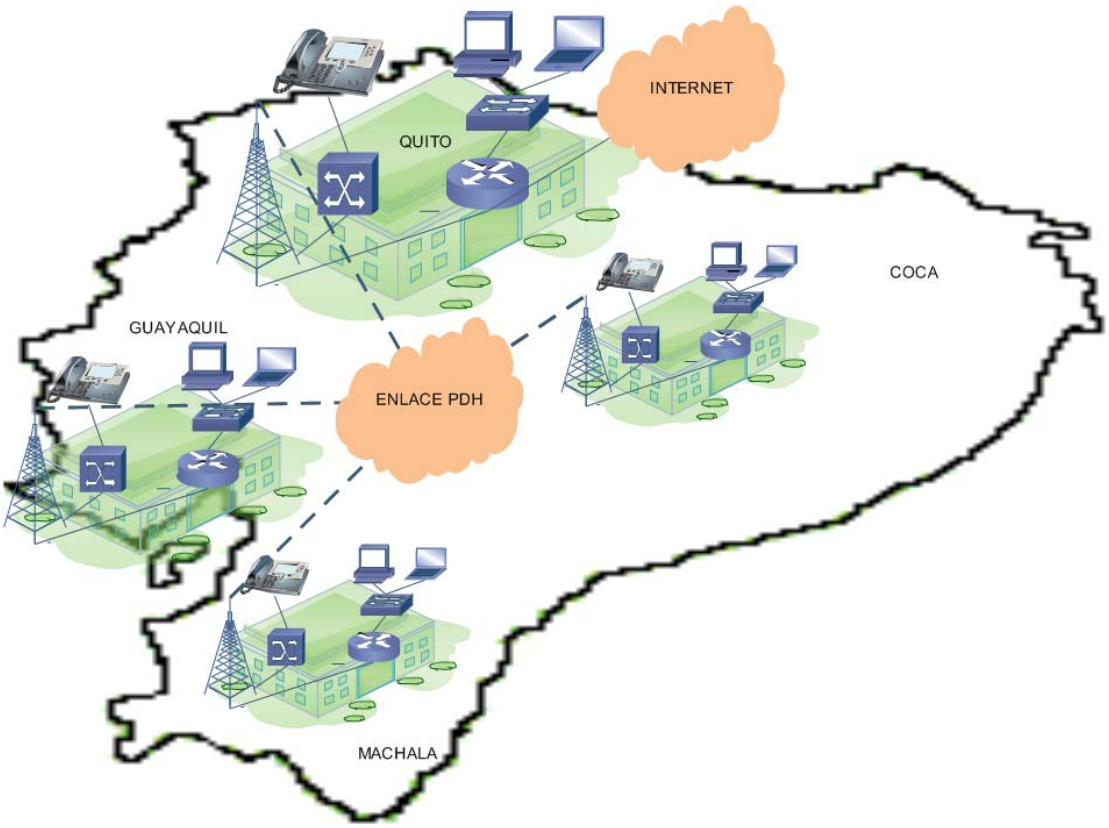

Figura 20. Arquitectura de la red de voz y datos de las Fuerzas Armadas

La Figura 21 describe la arquitectura física del nodo Quito existente. Los otros nodos tienen arquitecturas similares en lo que respecta a la arquitectura LAN. En cada mesa de trabajo que pertenece a cada uno de los nodos se encuentran puertos RJ-45 para las comunicaciones de datos, y puertos RJ-11 que pertenecen a la red de voz correspondiente a la telefonía conmutada. Con el desarrollo de una solución IPT serán necesarios solo puertos RJ-45, los mismos que son requeridos para ambos tipos de comunicación de voz y datos.

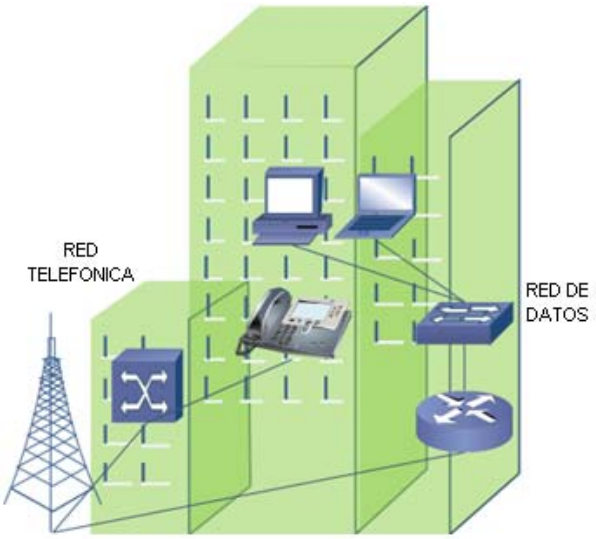

Figura 21. Arquitectura física de la red LAN en un nodo

La arquitectura de la red de voz mostrada anteriormente en la Figura 20 presenta las centrales de conmutación ubicadas en los nodos principales; y luego una estructura de telefonía donde todas las llamadas son originadas de forma individual y enrutadas vía conmutación de circuitos.

La red de comunicaciones de las Fuerzas Armadas comúnmente usa aplicaciones de e-mail, transferencia de archivos, aplicaciones web y otras. Una aplicación de tiempo no real en la red requiere priorización de tráfico. De cualquier forma las políticas de QoS y la configuración deben asegurar que el rendimiento de la aplicación existente no se degrade.

El servicio telefónico deberá soportar las siguientes funciones:

- Transferencia de llamada de un usuario de la red IPT a otro dentro de la red IPT o fuera de la misma

- Recuperar una llamada que está en espera desde cualquier punto de la red
- Recuperar una llamada que está timbrando en un punto de la red desde otro punto de la misma red
- Determinar restricciones de clase (CoR), en función de la ubicación o nivel del usuario
- Redireccionamiento de llamadas, por ejemplo fuera de las horas laborables sean redestinadas al lobby
- Llamada en espera
- Teléfonos que permitan desplegar un historial de las llamadas recibidas

4.2 REQUERIMIENTOS TÉCNICOS DEL CLIENTE

A continuación se detallan ciertas limitaciones que deberán ser consideradas en el diseño de la red:

- El tiempo de uso y las fallas permanentes de los equipos en uso
- La limitación en la escalabilidad de tarjetas en los slots
- Nivel de Retardo en la red

La red debe permitir una expansión rápida, en función de la demanda; es decir, el sistema de procesamiento de llamada debe ser ágilmente escalable y para ello debe:

- Requerir mínimo diseño en caso de expansión
- Proveer redundancia y balanceo de carga
- Optimizar el empleo del ancho de banda en el enlace WAN para el tráfico de voz

- En caso de fallas del enlace WAN, el control de llamada y el procesamiento de llamada local debe mantenerse

Con respecto a los teléfonos IP, los mismos deberán ser categorizados en 3 tipos:

- Teléfonos para los empleados y salas de estar
- Teléfonos a nivel gerencial y asistentes, con capacidad de multilínea y manos libres
- Teléfonos para video conferencia

Cada localización requerirá un **gateway** de voz para conectar a la telefonía local PSTN y deberá soportar un enlace troncal E1 PRI. Además cada lugar enrutará llamadas locales vía conexión PSTN, que terminarán en un gateway local.

Los Gateways de las ramas remotas deberán tener la funcionalidad de procesamiento-llamada para conectarse en caso de falla del enlace WAN.

Los teléfonos IP que están conectados a los gateways de voz locales deberán usar como primera opción los recursos de conferencia local.

El gateway deberá tener la capacidad de poder manejar Fax sobre IP a través de la red; por lo que será necesario que el gateway de voz tenga puertos análogos para conectar máquinas de fax.

Se requiere alta calidad de voz para la red IP. La integración de la red de voz y de datos requiere una infraestructura de red inteligente que pueda interpretar de forma adecuada la QoS en los terminales IP.

Por el momento, las Fuerzas Armadas no requieren la implementación del servicio de mensajería y correo de voz para la red telefónica IP, porque para esta funcionalidad se dará uso a la estructura de red existente.

La red requerirá lo siguiente:

- Terminales que puedan marcar tramas y paquetes en tiempo real para QoS.
- Una infraestructura que dé preferencia a tramas marcadas.

A pesar del bajo costo de la llamada local y llamada nacional será importante el **ruteo de llamadas** locales IP-WAN. Los siguientes son los requerimientos en el ruteo de las llamadas en el nuevo sistema IPT:

- Las llamadas deberán ser enrutadas vía IP-WAN como primera opción siempre y cuando haya la disponibilidad de medios, y luego vía enlace troncal PSTN si no hubiera ancho de banda disponible o el enlace WAN hubiera fallado.
- Solución automática de fallas deberá ser provista para todo el enlace IP WAN.
- El numero de dígitos a emplearse en las comunicaciones dentro de cada nodo y entre nodo será de 5 dígitos.
- No se podrá habilitar TEHO (Tail-end Hop-Off), bypass.

Los sitios remotos en cada enlace deberán usar los gateways locales para enrutar las llamadas locales y emplear los gateways de los nodos centrales como una alternativa en caso que la conexión local no esté disponible.

Se deberá incluir un mecanismo para controlar el número de llamadas que viaja a través del enlace IP-WAN.

La CoR (Restricción en función de la clase) deberá ser implementada en función del tipo de teléfono y la función que se le dará al mismo.

Para las llamadas de emergencia desde los lugares remotos o cualquier otro sitio, la llamada deberá ser enrutada vía PSTN a fin de que sea recibida en forma inmediata por el servicio local de ayuda. Esto evitará que una llamada sea enrutada por error vía TEHO y sea contestada por un sitio de auxilio distante.

4.3 CARACTERÍSTICAS, APLICACIONES Y SEGURIDADES EN LA RED IPT

La red actual tiene ciertas limitaciones propias del tipo de implementación que se llevó a cabo, y es por ello que se ha requerido de características adicionales y aplicaciones que no fueron posibles ejecutar en la red anterior.

Se requerirá de:

- Una Consola de atención manejada por un operador para cada lugar, este permitirá que se puedan contestar las llamadas locales y direccionarlo al usuario requerido
- Características de Asistencia Gerencial permitiendo recibir y transferir llamadas a los diferentes gerentes
- Servicios multilínea en los teléfonos, ya que es importante en los centros de llamada donde se emplea una línea para recibir llamadas y otra para poder realizar llamadas
- Movilidad para ciertos usuarios que luego de un proceso de registro en cualquier teléfono y personalizar su número telefónico, velocidad de llamada, etc. permita al usuario trabajar y recibir llamadas desde cualquier teléfono como si estuviera en la oficina
- Aplicaciones de Telefonía Virtual (Softphone), que serán instaladas sobre un computador de escritorio o laptop y así emular un teléfono IP real. Este tipo de aplicación es útil para usuarios que requieren movilidad

Con respecto a la **disponibilidad,** ésta juega un rol crítico para alcanzar los estándares deseados, ya que al integrar una solución de voz y datos el servidor del procesador de llamadas y los puntos finales de telefonía, tales como gateways, teléfonos IP o recursos de medio serán parte de la red de datos.

Además se requiere que esta solución provea redundancia y tolerancia a las fallas. Una falla en el servidor, gateway, gatekeeper, switch u otro equipo no debe afectar a los usuarios.

La solución IPT debe proveer una disponibilidad de servicio del 90%.

4.4 CONDICIONANTES A LOS PROVEEDORES

Una vez que se ha generado la RFP se espera que los proveedores propongan una combinación de:

- Servidores de aplicación
- Servidores de control de llamada
- Gateways
- Dispositivos de usuario y de conferencia

Los proveedores utilizarán equipos Cisco, tanto en hardware y software.

Esta RFP intenta proveer una base para poder evaluar alternativas de sistemas de comunicación y permitir al proveedor generar una solución flexible y apropiada con el mejor costo-beneficio.

Las Fuerzas Armadas se reservan el derecho de modificar los requerimientos del sistema añadiendo o eliminando equipos específicos o características opcionales.

Las Fuerzas Armadas se reservan el derecho de mantener o modificar el enlace WAN existente.

El proveedor deberá usar todo su conocimiento y experiencia dentro de la industria de las comunicaciones para recomendar una solución creativa que cumpla los requerimientos que se piden en esta RFP.

Se dará preferencia al proveedor que provea el diseño más comprensible, mejor capacidad futura y mejor soporte post venta.

Se dará preferencia a las compañías de carácter local y con certificaciones en telefonía IP, así como una certificación en Cisco Systems y/o 3com Corporation.

Como ya se mencionó, la información descrita en el RFP se desarrolló con la guía del Ing. Wilson Freire, con quien se estableció un diálogo constante para lograr un trabajo que pudiera seguir un mismo conjunto de reglas, requerimientos, planificación e información, y gracias a ello se pudo realizar las preguntas e interpretaciones adecuadas que permitieron la construcción de la RFP. La Tabla VIII provee la información de este contacto.

Tabla VIII. Información de contacto

Nombre de contacto:	Ing. Wilson Freire
Dirección:	Base Naval Sur
Teléfono:	593 – 4 – 2500230
Dirección de e-mail:	wilsonfr2002@hotmail.com

4.5 INFRAESTRUCTURA DE ENERGÍA

En la red de datos de las Fuerzas Armadas se implementará una infraestructura de energía separada de la red de datos, es decir, no se diseñará poder en línea o PoE y los equipos a emplearse no contarán con esta característica con el objetivo de reducir los altos costos que implica equipos con esta particularidad. Los teléfonos IP serán alimentados por una red eléctrica individual.

4.6 CUESTIONARIO PARA EL ANÁLISIS DE LA RED ACTUAL

El cuestionario que se muestra a continuación brinda información acerca de la estructura actual con que cuenta la red de comunicaciones de las Fuerzas Armadas actualmente.

Tabla IX. Generalidades de la empresa

No.	Pregunta	Respuesta
1	Nombre del Cliente	COMACO
2	Breve descripción de la empresa	Militar
3	Provea una breve visión general de los servicios y aplicaciones que el cliente opera en la red	Voz, aplicaciones de las FF.AA.
4	Identifique si la implementación es de una nueva red. Si no, dé un breve resumen de la red actual	Existe un backbone, distribución y accesos de las diferentes fuerzas.

Tabla X. Diseño de la Red - Jerarquía

No.	Pregunta	Resp
1	¿Tiene la red un núcleo separado, distribución y capas de acceso que son apropiadas para el número de usuarios del campo?	■ Sí □ No
2	¿Están los usuarios, servidores y servicios de WAN conectados a la capa de acceso para todos los ambientes del campo?	■ Sí □ No

3	Si existe un ambiente de campo distribuido, ¿Soporta la red un núcleo de WAN jerárquico y modular con núcleo definido, distribución y conectividad de acceso?	■ Sí □ No

Tabla XI. Diseño de Red - Modularidad

No.	Pregunta	Resp
1	¿Tiene la red módulos de hardware y software consistentes implementados para el servidor de LAN y el acceso de usuario?	■ Sí □ No
2	¿Tiene la red módulos de hardware y software consistentes implementados para la distribución de LAN y las capas de núcleo?	■ Sí □ No
3	¿Tiene la red módulos de hardware y software consistentes implementados para las capas de acceso y distribución de servicios WAN?	■ Sí □ No

Tabla XII. Diseño de Red - Desempeño de la Capa de núcleo

No.	Pregunta	Resp
1	¿Es posible incrementar la capacidad del núcleo?	■ Sí □ No
2	¿Tienen los dispositivos de capa de núcleo los recursos de sistema requeridos, incluido aplicación de tarjeta madre, capacidad de reenvío de paquetes, memoria y CPU para soportar fallas de núcleo redundante, y convergencia rápida de Capa 2 y Capa 3?	□ Sí ■ No
3	Si un núcleo de capa 2 se utiliza, ¿tiene capacidad de crecer a capa 3?	■ Sí □ No

Tabla XIII. Diseño de Red - Alta disponibilidad de la capa de núcleo

No.	Pregunta	Resp
1	¿Soporta el núcleo del campo dispositivos de las capas de núcleo redundantes y modulares?	■ Sí □ No
2	¿Existen en el núcleo del campus caminos de capa 3 de igual costo para convergencia de ruteo óptimos?	■ Sí □ No
3	¿Están los dispositivos de capa de núcleo ambientalmente controlados y protegidos en energía para más alta disponibilidad?	□ Sí ■ No

Tabla XIV. Diseño de Red - Configuración de la Capa de núcleo

No.	Pregunta	Resp
1	¿Los enlaces entre los dispositivos de la capa de núcleo y los dispositivos de la capa de distribución están configurados para igualar las configuraciones de velocidad y dúplex?	■ Sí □No
2	Si se utiliza un núcleo de capa 3, ¿Las interfases están configuradas con subredes de punto a punto?	□ Sí ■ No

Tabla XV. Diseño de Red - Desempeño de la Capa de Distribución

No.	Pregunta	Resp
1	¿Se ha incrementado el ancho de banda de la capa de distribución para manejar escalabilidad de acceso, agregación de acceso y solución automática de falla de distribución?	■ Sí □ No
2	¿Los dispositivos de capa de distribución tienen suficientes tarjetas madres, CPU y recursos de memoria para la conmutación multicapa y para las características requeridas (incluido el Hot Standby Routing Protocol [HSRP])?	□ Sí ■ No
3	¿Los dispositivos de capa de distribución tienen los recursos requeridos para soportar parámetros QoS del campus LAN implementado en la capa de distribución?	■ Sí □ No

Tabla XVI. Diseño de la Red - Alta disponibilidad de la Capa de distribución

No.	Pregunta	Resp
1	¿La capa de distribución tiene dispositivos redundantes que pueden manipular los requerimientos de ancho de banda cuando la conectividad de la distribución alterna o primaria no está disponible?	□ Sí ■ No
2	¿La organización tiene solución automática de falla anticipada y escenarios de recuperación con los protocolos de ruteo elegidos, HSRP y configuración de expansión en árbol?	□ Sí ■ No
3	¿El trunking entre los dispositivos de la capa de distribución es configurado solo para VLANs, donde los servidores de acceso de alta disponibilidad son necesitados para switches de acceso múltiple?	■ Sí □ No

Tabla XVII. Diseño de Red - Arquitectura VLAN de la Capa de distribución

No.	Pregunta	Resp
1	En general, ¿las VLANs están solamente implementadas en dos switches de la capa de distribución y un switch de la capa de acceso, y no son llevadas en algún enlace entre los switches de la capa de distribución?	□ Sí ■ No

2	¿Están limitadas las VLANs a dos dispositivos de capa de distribución y dos dispositivos de capa de acceso donde son necesarios accesos de gran disponibilidad?	□ Sí ■ No

Tabla XVIII. Diseño de Red - Configuración de la Capa de Distribución

No.	Pregunta	Resp
1	¿La expansión en árbol está configurada en los switches de distribución, aún cuando los lazos no están planificados?	■ Sí □ No
2	¿Están configurados los dos switches de distribución como raíces alternas y raíces secundarias para VLANs alternas, con los routers HSRP activo y HSRP en standby según corresponda, para dar equilibrio y redundancia?	□ Sí ■ No

Tabla XIXX. Diseño de Red - Características de la Capa de Acceso

No.	Pregunta	Resp
1	¿La capa de acceso soporta conexiones conmutadas de 10/100 Mbps para todos los usuarios de estaciones terminales?	■ Sí □ No
2	¿La capa de acceso soporta conexiones conmutadas de 100 o 1000 Mbps para todas las conexiones de servidor y de distribución?	■ Sí □ No
3	¿El dispositivo de capa de acceso soporta múltiples colas para priorizar tráfico de voz donde sea necesario?	■ Sí □ No
4	¿Los dispositivos de capa de acceso pueden manejar utilización de nivel máximo de servidores y clientes?	■ Sí □ No

Tabla XX. Diseño de Red - Alta disponibilidad de la Capa de acceso

No.	Pregunta	Resp
1	¿Los switches de acceso tienen trunking redundante a dos switches de distribución y solo a ellos?	■ Sí □ No
2	¿Los switches de acceso más importantes tienen procesador y alimentación redundante?	■ Sí □ No
3	¿Los servidores de alta disponibilidad tienen conexiones redundantes en una VLAN por dos switches de acceso?	■ Sí □ No
4	¿Está configurada la auto-negociación para los clientes?	□ Sí ■ No

5	¿Han sido unificadas el dúplex y la relación de velocidad para conexiones de servidor?	■ Sí □ No
6	¿El PortFast está configurado en puertos cliente/servidor?	■ Sí □ No
7	¿Está configurado el UplinkFast en switches que soportan servidores de alta disponibilidad, donde el reenvío y el bloqueo de enlaces troncales VLAN existen en el switch de acceso?	■ Sí □ No

Tabla XXI. Diseño de Red - Diseño de WAN y alta disponibilidad

No.	Pregunta	Resp
1	¿Tiene usted una topología de red en estrella?	■ Sí □ No
2	¿Tendrá la WAN enlaces redundantes para soportar alta disponibilidad en la WAN?	■ Sí □ No

Tabla XXII. Diseño de Red - Lineamientos básicos de la WAN

No.	Pregunta	Resp
1	¿Usted recolecta lineamientos básicos para su WAN (proyectado a soportar telefonía IP) que incluye utilización del enlace, profundidad de cola, retardo de paquete de extremo a extremo, CPU y memoria?	■ Sí □ No
2	¿La empresa ha determinado el impacto potencial del tráfico VoIP en la WAN en términos de utilización del ancho de banda y recursos del sistema?	□ Sí ■ No
3	¿Los lineamientos básicos actuales y el tráfico añadido sugieren que el uso y los recursos de sistema están bien dentro de las capacidades de la red, incluyendo uso del enlace en máximo nivel por debajo del 75% y enlaces WAN con un mínimo de 128 Kbps?	■ Sí □ No

Tabla XXIII. Diseño de Red - Planificación de Capacidad de la WAN

No.	Pregunta	Resp
1	¿La WAN será mejorada para soportar soluciones IPT para asegurar el desempeño de voz consistente?	■ Sí □ No
2	¿Los enlaces WAN que soportan tráfico de voz tendrán los requerimientos de ancho de banda mínimo para el despliegue de la IPT? (paquetes de 64 Kbps, línea alquilada de 64 Kbps, o ATM de 768 Kbps o es requerido ATM/Frame Relay)	■ Sí □ No

3	¿La WAN tendrá el ancho de banda adecuado para soportar utilización de voz a nivel máximo a través de la WAN?	■ Sí □ No

Tabla XXIV. Diseño de Red - Direccionamiento IP

No.	Pregunta	Resp
1	Provea información del esquema actual de direccionamiento IP	
2	¿Su organización tiene un plan de direccionamiento IP para integrar teléfonos IP en la red?	□ Sí ■ No
3	¿La empresa tiene planes para implementar RFC 1918 para direccionamiento privado?	□ Sí ■ No
4	¿El plan de direccionamiento IP soporta reportes de dirección IP?	□ Sí ■ No

Tabla XXV. Diseño de Red - Protocolo de Enrutamiento IP

No.	Pregunta	Resp
1	¿La empresa ha implementado el protocolo Open Shortest Path First(OSPF) o Enhanced Interior Gateway Routing Protocol (EIGRP) para una convergencia mejorada de la red?	■ Sí □ No
2	¿La empresa usa algún otro protocolo de enrutamiento que redistribuya hacia/desde los sistemas autónomos EIGRP o OSPF?	□ Sí ■ No
3	¿La empresa mantiene configuraciones de protocolo de enrutamiento estándar para todos los routers en la red?	■ Sí □ No
4	¿Las rutas estáticas están limitadas a bordes de red para conectividad asociada o copia de respaldo ISDN?	□ Sí ■ No
5	¿La empresa ha implementado reporte de IP hacia el núcleo para reducir el overhead del protocolo de enrutamiento y asegurar escalabilidad IP?	□ Sí ■ No
6	¿La empresa ha implementado aplicaciones para depuración o enrutamiento por defecto en ambientes WAN de topología en estrella para reducir el overhead de protocolo de enrutamiento en enlaces WAN?	□ Sí ■ No
7	¿La empresa ha revisado el impacto del protocolo de enrutamiento y la escalabilidad basado en los tipos de dispositivo, número de rutas y protocolos de enrutamiento IP vecinos?	□ Sí ■ No

8	¿El enrutamiento está deshabilitado en interfases de usuario y servidores de LAN para prevenir enrutamiento de núcleo a través de usuarios de LAN?	□ Sí ■ No
9	¿El enrutamiento es filtrado en sitios de acceso de interfases WAN para publicar solo información del sitio WAN?	□ Sí ■ No
10	¿Qué otros protocolos de enrutamiento son utilizados en la red además del protocolo IP?	Listar: OSPF EIGRP

Tabla XXVI. Diseño de Red - HSRP de IP

No.	Pregunta	Resp
1	¿La red utiliza HSRP para el soporte del gateway redundante por defecto?	■ Sí □ No
2	¿La empresa comprende asuntos de convergencia dado el número de los grupos HSRP soportados en el dispositivo?	■ Sí □ No
3	¿La red utiliza la característica de tener predominancia sobre HSRP para devolver el control al gateway primario, cercanamente asociado con la raíz de expansión en árbol para la VLAN?	■ Sí □ No
4	¿Tiene la empresa considerada la característica de monitoreo de HSRP que es usado para monitorear el backbone o la conectividad del WAN desde el gateway HSRP primario?	■ Sí □ No

Tabla XXVII. QoS Calidad de Servicio

No.	Pregunta	Resp
1	¿Pueden utilizarse para voz VLANs auxiliares con IEEE 802.1Q/p?	■ Sí □ No
2	¿Los flujos de portadora de voz pueden ser marcados como EF (Expedited Forwarding (Envío Acelerado)) y flujo de control de voz como AF31 (Assured Forwarding 31 (Envío asegurado 31))/CS3 (Class Selector 3)?	■ Sí □ No
3	¿La QoS es configurable en dispositivos en el que los búffers podrían estar alcanzando capacidad?	■ Sí □ No
4	¿El Encolamiento de Baja Latencia (LLQ, Low Latency Queuing) es configurable en todas las interfases WAN?	■ Sí □ No

5	¿Tiene usted algún tráfico adicional importante aparte de la voz (como video, DLSW, etc.)? Si la respuesta es afirmativa, por favor, especifique los tipos de tráfico y cómo están actualmente clasificados en su red.	■ Sí □ No

Tabla XXVIII. Servicios de red DNS

No.	Pregunta	Resp
1	¿La empresa tiene una arquitectura DNS flexible con servidores DNS primarios y secundarios?	□ Sí ■ No
2	Provea las direcciones IP del servidor DNS y su nombre de dominio completamente calificado	□ DNS 1 _____No aplica_____ □ DNS 2 _____No aplica_____ □ FQDN _____No aplica_____

Tabla XXIX. Detalles de implementación DHCP

No.	Pregunta	Resp
1	¿La empresa utiliza los servicios DHCP para proveer el direccionamiento IP para clientes?	□ Sí ■ No
2	¿Qué software DHCP (incluya el número de la versión) está en uso?	□ MS DHCP □ Lucent QIP □ Otro Especifique _____No aplica_____
3	¿El servidor DHCP soportará la configuración de opciones personalizadas? (Los teléfonos IP aceptan la información del servidor TFTP en la opción 150, que provee direcciones IP de una lista de servidores TFTP; o 66 de DHCP, que provee dirección IP de un solo servidor TFTP)	□ Sí □ No
4	Si la respuesta a la pregunta 3 es afirmativa, puede la red IPT usar su servidor DHCP existente para proveer las direcciones IP para puntos terminales IPT como los teléfonos IP y los gateways de voz?	□ Sí □ No
5	¿El servicio DHCP es flexible con los respaldos de configuración y la imagen del disco?	□ Sí □ No
6	¿Utiliza un servidor DHCP centralizado para toda la empresa?	□ Sí □ No
7	Si usted tiene servicios DHCP distribuidos en las regiones remotas, ¿el router provee los servicios DHCP o tiene un servidor DHCP separado para cada oficina regional?	Provea detalles en los comentarios de esta sección

Tabla XXX. NTP

No.	Pregunta	Resp
1	¿La empresa utiliza actualmente NTP?	□ Sí ■ No
2	Si la respuesta a la pregunta 1 es afirmativa, ¿cuáles son las direcciones IP de NTP de las fuentes de NTP?	□ Fuente 1 _____ □ Fuente 2 _____
3	¿Quiere usted configurar los dispositivos IPT para sincronizar sus relojes con los servidores NTP?	■ Sí □ No

Tabla XXXI. Directorios

No.	Pregunta	Resp
1	¿Qué servicio de directorio está actualmente desplegado en la empresa?	□ Microsoft AD □ Netscape □ Sun One □ iPlanet □ Version ■ Ninguno
2	¿Hay algún requerimiento para integrar aplicaciones IPT con su directorio corporativo existente?	□ Sí ■ No
3	Si la integración de directorio no es un requerimiento, ¿Está considerando proveer la búsqueda del acceso de directorio corporativo de los teléfonos IP?	□ Sí ■ No

Tabla XXXII. Sistema de Mensaje

No.	Pregunta	Resp
1	¿Cuál es el ambiente actual de mensajería de correo electrónico utilizado en la empresa?	□ Ms Exchange □ Lotus Domino □ Other □ Version ■ Varios
2	¿La empresa se proyecta a desplegar mensajería unificada junto al despliegue de la telefonía IP?	□ Sí ■ No

Tabla XXXIII. Cableado y Enlaces de red

No.	Pregunta	Resp
1	¿La empresa sigue lineamientos comunes para instalaciones de cableado de par trenzado de Categoría 5?	■ Sí □ No
2	¿La empresa mantiene patch cords bien organizados y etiquetamiento de cables para cables WAN, fibra y cobre?	□ MS DHCP □ Lucent QIP □ Otro ■No tiene
3	¿Están el cableado de fibra y de cobre probados?	■ Sí □ No
4	¿Están el cableado de fibra y de cobre probados?	■ Sí □ No
5	¿La empresa tiene segmentos no Ethernet en la red?	□ Sí ■ No

Tabla XXXIV. Escalabilidad de hardware

No.	Pregunta	Resp
1	¿Existen switches de distintos proveedores en la capa de acceso de la red?	■ Sí □ No
2	¿Necesita conectar los teléfonos IP a los switches de acceso que son de distintos proveedores?	■ Sí □ No
3	Si usted tiene switches de diferentes proveedores, ¿soportan éstos IEEE 802.1Q/p?	■ Sí □ No
4	¿Qué estándar de Power over Ethernet (PoE) quiere utilizar la empresa?	□ IEEE 802.3af □ Otro ■ No se requiere
5	¿Pueden los switches en la capa de acceso ser mejorados para soportar poder en línea?	□ Sí ■ No
6	¿El hardware escalará para soportar los puntos finales IPT tales como teléfonos IP y gateways?	■ Sí □ No
7	¿Tiene la empresa redundancia de chasis donde es apropiado?	□ Sí ■ No
8	¿Tiene la empresa redundancia de módulo donde es apropiado?	□ Sí ■ No
9	¿La empresa tiene piezas de repuesto de hardware en el sitio?	■ Sí □ No

10	¿La empresa tiene un contrato de servicio con el proveedor de los equipos para reemplazar las partes defectuosas?	□ Sí ■ No

Tabla XXXV. Software

No.	Pregunta	Resp
1	¿La empresa crea y mantiene estándares de software de la red?	□ Sí ■ No
2	¿La empresa tiene un proceso de certificación de software en su lugar?	□ Sí ■ No
3	¿El software es probado antes de que sea desplegado en la red de producción?	□ Sí ■ No
4	¿La empresa estandariza el software de despliegue general donde sea posible?	□ Sí ■ No
5	¿La empresa mantiene configuraciones estándares de software globales?	□ Sí ■ No

Tabla XXXVI. Protección de energía

No.	Pregunta	Resp
1	¿Los dispositivos de capa de núcleo y capa de distribución que sirven a los edificios o sectores de energía protegidos están protegidos con UPS y generador de respaldo?	■ Sí □ No
2	¿Los switches de acceso están protegidos con UPS o generadores donde las redes de acceso están protegidos o donde la telefonía IP se requiere?	■ Sí □ No
3	¿La empresa usa componentes de red que soportan suministros de poder redundantes?	■ Sí □ No
4	¿La empresa desempeña mantenimientos periódicos en los UPS y generadores para asegurar la disponibilidad del sistema?	■ Sí □ No

Tabla XXXVII. Condiciones ambientales

No.	Pregunta	Resp
1	¿La empresa investiga información sobre disipación de calor, temperatura y humedad para los nuevos productos?	□ Sí ■ No

2	¿La empresa provee ventilación y enfriamiento ininterrumpido para los dispositivos de red para mantener una temperatura y ambiente consistente de operación?	■ Sí □ No
3	¿La organización utiliza sistemas de monitoreo ambientales para las ubicaciones de equipos importantes?	□ Sí ■ No
4	¿El cuarto de servidor donde usted está planeando ubicar los servidores de IPT, switches y gateways tiene suficientes espacios en los racks?	■ Sí □ No
5	¿Tiene su empresa tomas de salida de poder adecuadas para soportar los dispositivos adicionales?	■ Sí □ No
6	¿Puede el sistema de UPS existente manejar la carga adicional para soportar los nuevos servidores IPT, gateways y switches?	■ Sí □ No

Tabla XXXVIII. Seguridad

No.	Pregunta	Resp
1	¿La empresa ha desarrollado una política de seguridad con respecto al acceso a los dispositivos de la red, monitoreo, privacidad y protección de valores de información?	■ Sí □ No
2	¿La empresa ha implementado medidas básicas de seguridad tales como claves más seguras y encriptación de claves para el control de acceso de los dispositivos por la red?	□ Sí ■ No
3	¿Los dispositivos de la red están en una ubicación segura que requiere autorización para el acceso físico?	□ Sí ■ No
4	¿Hay un mecanismo empleado para autenticar usuarios, control de acceso a los dispositivos de la red y proveer información de contabilidad para propósitos de auditoria?	□ Sí ■ No
5	¿Qué antivirus utiliza la empresa para proteger los servidores y estaciones de trabajo de los virus?	□ McAfee ■ Symantec □ Trend Micro □ Other
6	¿La empresa usa actualmente algún host de detección de intruso/software de prevención?	□ Sí ■ No
7	¿La empresa tiene una política definida para la aplicación de soluciones de seguridad y parches de sistema operativo para servidores críticos? Si es afirmativo, describa en los comentarios. Incluya información tal como qué tanto tiempo tomará hacer un arreglo, qué procedimientos de prueba/certificación se siguen, etc.	□ Sí ■ No

5. FASE DE PLANIFICACIÓN DE LA RED IP REQUERIDA EN LA SOLICITUD DE PROPUESTA RFP

Es importante como primer punto de la fase de planificación de la tesis entender las expectativas de negocio, técnicas y requerimientos de la futura red IPT; por lo que se ha recolectado la información correspondiente a la empresa para la cual estamos desarrollando este diseño, la red de datos de las Fuerzas Armadas.

5.1 Generalidades de la Red de Fuerzas Armadas

Las Fuerzas Armadas tienen a su cargo una red de comunicaciones de uso exclusivo, siendo el COMACO el encargado de su administración y mantenimiento. Los servicios que brinda son transmisión de datos y telefonía del tipo conmutación de circuitos.

En lo que respecta a la red de datos, en la actualidad, está constituida por un backbone, una red de distribución y una red de acceso a los diferentes repartos que constituyen las Fuerzas Armadas.

Los objetivos y planes del COMACO para la red de voz y de datos durante los siguientes 3 a 5 años es "*Analizar la viabilidad del diseño de una Red Convergente para optimizar la red existente".*

Las expectativas del COMACO, hemos clasificado de la siguiente manera:

- *Expectativas de solución*: La solución propuesta será efectiva permitiendo brindar un servicio de telefonía IP a los miembros de Fuerzas Armadas, optimizando el ancho de banda en el enlace PDH existente
- *Expectativas de proyecto*: La solución deberá contar con niveles de administración múltiples para que los técnicos en administración y operación puedan configurar de la red ágilmente
- *Expectativas económicas*: La red de comunicaciones que se va a diseñar no tiene fines lucrativos debido a su uso militar. Con esta nueva red no se pretende generar ningún ingreso de dinero, sino la reducción de costos operativos, el mejoramiento de la productividad y la eficiencia del trabajo

5.2 Aspectos a considerarse en la nueva red de las Fuerzas Armadas

La red es de **carácter jerárquico**; ya que agrupa terminales de usuario y centros de conmutación en grupos ordenados de modo que cada uno de ellos dependa de uno y sólo uno de categoría inmediatamente superior. La red jerárquica existente permite usar caminos redundantes y rutas óptimas facilitando la separación de dominios de broadcast; además permite una rápida comprensión de la red al momento de dar soporte. Esta red tiene sus capas de núcleo, distribución y acceso

debidamente separadas y el número de usuarios para cada campo es el apropiado. En todos los sitios a los que llega la red de datos, los usuarios, servidores y servicios WAN están conectados a la capa de acceso. La red soporta un núcleo WAN jerárquico; tiene un núcleo definido, distribución y acceso.

La red de datos de las Fuerzas Armadas brinda un diseño **modular**; ya que cuenta con módulos de hardware y software consistentes para servidores LAN y acceso de usuarios; para distribución de LAN y capas del núcleo; para capas de acceso y distribución de servicios WAN. La modularidad facilitará la ampliación o el cambio de un sistema con las mínimas interrupciones para los usuarios; por lo tanto, permite brindar un mejor soporte, solucionar problemas y reemplazar de manera rápida los componentes descompuestos.

La primera capa en analizar es la **Capa de acceso**, donde los usuarios pueden acceder a la red. Esta se encarga de recolectar y acondicionar el tráfico que proviene de las estaciones de usuarios. Al hablar de esta capa, debemos empezar por la planificación de las VLANs en la red; para ello podemos tener múltiples VLANs en un switch. De limitar a una sola VLAN, se limitaría el árbol de expansión lo que da como resultado un incremento en el tiempo de convergencia.

Las consideraciones a tomar en cuenta en esta capa son:
Los teléfonos IP serán conectados en los switches de la capa de acceso. Algunos teléfonos IP Cisco tienen un puerto PC para conectar al teléfono las estaciones de trabajo. Deberemos entonces separar el tráfico que viene de los teléfonos IP con el

del tráfico de datos de las estaciones de trabajo mediante la característica de VLAN de voz, al que se le asociará una VLAN ID de voz. Esto es importante considerar ya que la calidad de sonido de una llamada por un teléfono IP puede deteriorarse si se envía junto con el tráfico de datos. El VLAN de voz permite soportar QoS basado en el estándar IEEE 802.1Q/p (Class of Service) que soporta prioridad de tramas.

Las ventajas de separar VLANs de voz y datos son:

- Tratar a los paquetes con distintos niveles de prioridad en los dispositivos de la red para garantizar la calidad de voz
- Asignación de direcciones IP de dispositivos voz que puedan diferenciarse de las direcciones IP de equipos para datos
- Facilitar el troubleshooting al diferenciarse fácilmente el tráfico de voz o datos
- Facilitar las decisiones de políticas de seguridad de la red para cada tipo de información
- Los teléfonos IP no tendrán que responder a los broadcasts generados por la red de datos

Para los switches de la capa de acceso que no poseen la característica de VLAN de voz, se deberá configurar esta característica de forma manual en cada uno de los teléfonos IP. También debemos recordar dos características muy importantes que deben poseer los switches a emplearse en la capa de acceso; estas son:

- Mínimo tiempo de inicialización de los teléfonos IP. Esta característica lo brinda CISCO a través de su característica PortFast.

- Capacidad de enlace rápido de la capa de acceso a la capa de distribución en caso de falla. Esta característica lo brinda CISCO a través de su característica *UplinkFast*

Otra capa importante es la **capa de distribución**, que agrupa los dispositivos de la capa de acceso. Una de las características más importantes de la capa de distribución es que es el punto en el que los terminales de dominio de capa 2 y el dominio de capa 3 empiezan, por lo que en esta capa se manejarán protocolos de capa 2 y de capa 3. Las características de la capa de distribución se definen de la siguiente manera:

- Agrupa swiches de la capa de acceso
- Las VLANs que se definen en el dominio de capa 2 terminan en esta capa
- Constituye el primer salto a un gateway para las estaciones terminales
- Provee servicios de seguridad, calidad de servicio y encolamiento
- Permite enlaces redundantes hacia la capa de núcleo
- Es en esta capa donde se encuentra la mayor parte de la inteligencia de la red

La capa de distribución de la red de datos de las Fuerzas Armadas cuenta con dispositivos redundantes para una completa disponibilidad de la red: un switch primario o máster y un switch secundario o de respaldo. Para obtener esta redundancia, además de requerir un switch duplicado para la capa de distribución, será necesario emplear métodos de tolerancia a fallos de la puerta de enlace o gateway por defecto de cara a los equipos. En este caso, se utiliza el HSRP de Cisco.

Cualquiera de las direcciones IP de los routers virtuales puede utilizarse como el router por defecto del primer salto para los terminales.

La ventaja al utilizar HSRP en la red es una mayor disponibilidad de caminos por defecto sin requerir las configuraciones de enrutamiento dinámico o CDP en cada Terminal.

Los lineamientos que seguiremos para la capa de distribución son:

- Utilizar OSPF para mejorar la convergencia de la red
- Seguir estándares de configuración consistentes y convenciones de nombres en todos los routers para mejor convergencia y facilidad para solución de problemas
- Implementar *IP SUMMARIZATION* (Optimización en el empleo de direcciones IP) hacia el núcleo para reducir la información de enrutamiento del Paquete IP; de esta manera aseguramos la escalabilidad IP
- Implementar enrutamiento por defecto en los ambientes de topología en estrella de la WAN; de esta forma reducimos la información de enrutamiento y control del paquete IP.

La última capa que debemos considerar en la red es la **capa de núcleo**, que dentro del modelo de diseño tiene dos tareas importantes:

- Interconectar todos los bloques de la capa de distribución
- Reenviar todo el tráfico tan rápido como sea posible

Las características del funcionamiento de la capa de núcleo son:

- Agregar capas de distribución para formar una red interconectada
- Proveer tráfico a alta velocidad entre las capas de distribución
- Proveer un ambiente de enrutamiento IP flexible

La capa de núcleo está basada en protocolos de capa 3. En esta capa se debe tener la precaución de no configurar servicios como seguridad, control de acceso o cualquier actividad que implique procesamiento de paquetes, debido a que su función debe ser proveer velocidad.

La capa de núcleo en la red actúa como una capa transitoria. Los switches de la capa de acceso no deben ir conectados directamente a la capa de núcleo. En la capa de núcleo existe redundancia en los enlaces que conforman la red WAN, como se puede observar en la Figura 22.

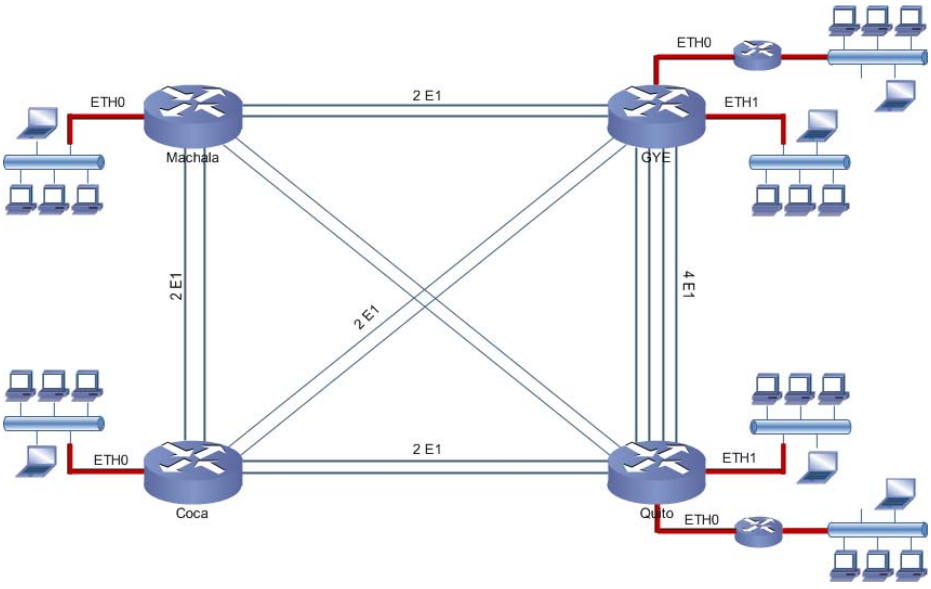

Figura 22. Infraestructura de la capa de núcleo en la red

Al revisar la infraestructura de la red, respecto a los **lineamientos comunes a las diferentes capas,** hay que asegurarse que haya redundancia en cada una de ellas y utilizar versiones de software estándar en la red, para evitar situaciones en las cuales fallas de hardware o software impacten a la red.

Es de suma importancia evitar en lo posible puntos de falla únicos en la red. En la capa de acceso, habrá un punto único de falla en caso que un teléfono IP no esté conectado a dos switches diferentes.

En la capa de distribución debemos asegurarnos de mantener la modularidad de la red; por lo tanto conectaremos diferentes módulos en los diferentes servicios que se brindan (manteniéndolos separados), como se muestra en la Figura 23; En la figura se observa la red de Internet, la red PSTN, la red de datos, la red de telefonía IP, el CallManager, solución CISCO basado en un software para la gestión de las llamadas, y las estaciones de trabajo de los usuarios; todas estas redes están conectados a sus propios switches de acceso. Los switches de acceso tienen conexión a cada uno de los switches de la capa de distribución para asegurar la redundancia de la capa. Los switches de distribución de cada módulo tienen conexiones dobles hacia los switches de capa 3. Esta estrategia provee una arquitectura robusta, de gran disponibilidad y facilidad de solución de problemas; propia de una red de Fuerzas Armadas.

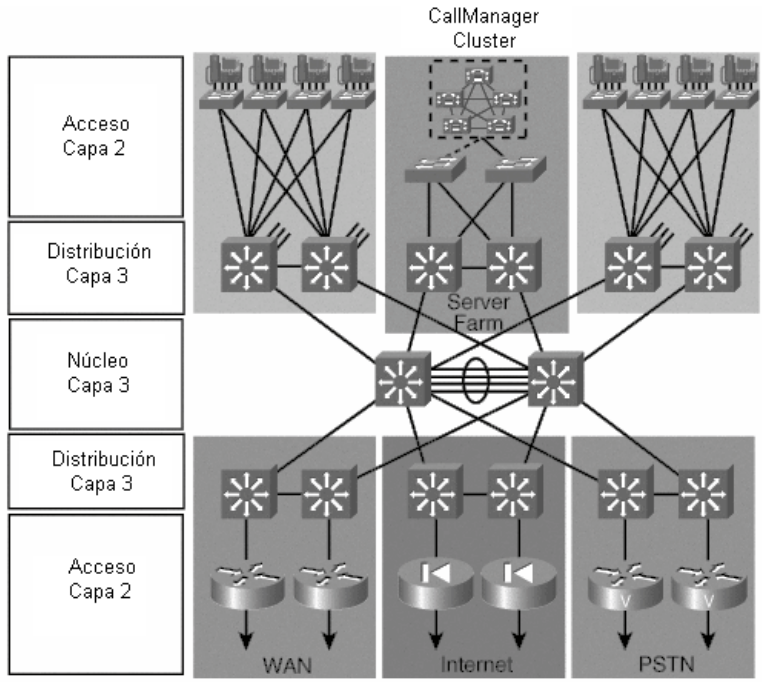

Figura 23. Arquitectura de la red modular

5.3 Infraestructura de WAN

Para brindar calidad de voz en el tráfico de la WAN, debemos rediseñar la red para que soporte QoS y Control de Admisión de Llamada (CAC) ya que por ser no orientado a conexión, sin un control se aceptarían tantas comunicaciones como se soliciten, resultando en una degradación de la calidad de voz. Para evitar el exceso de suscriptores en el enlace, se utilizará CAC en el transporte del tráfico de voz.

En la topología de la red deberemos asegurarnos realizar el diseño de manera que no sobre-suscribamos los enlaces. La topología de malla parcial o total no puede brindar el control para el despliegue de CAC y QoS. La tecnología WAN disponible en la red de datos es PDH, la misma que permitirá garantizar calidad de voz.

Tabla XXXIX. Características WAN de la red de las Fuerzas Armadas

Enlace	Equipo de WAN (Switch-Router)	Velocidad/Tipo	Utilización actual	CIR
Quito – Guayaquil	CISCO 6500	8 Mbps, PDH	50%	8 Mbps
Quito – Coca	CISCO 6500	2 Mbps, PDH	50%	2 Mbps
Quito – Machala	CISCO 6500	2 Mbps, PDH	50%	2 Mbps
Guayaquil – Machala	CISCO 6500	2 Mbps, PDH	50%	2 Mbps
Guayaquil – Coca	CISCO 6500	2 Mbps, PDH	50%	2 Mbps
Machala – Coca	CISCO 6500	2 Mbps, PDH	50%	2 Mbps

5.4 Calidad de Servicio en la Infraestructura del Backbone

La pérdida de paquetes, el retardo de una vía y el jitter afectan la QoS. Estos parámetros son muy importantes en un ambiente WAN. Aplicaremos algunas técnicas para reducir estos parámetros en el circuito:

- Minimización del retardo
- Utilización de modelación de tráfico
- Aprovisionamiento de ancho de banda de la WAN
- Utilización de compresión de voz

El objetivo de la **minimización del retardo** es alcanzar la recomendación ITU G.114. Los componentes que introducen retardo se ilustran en la Figura 24:

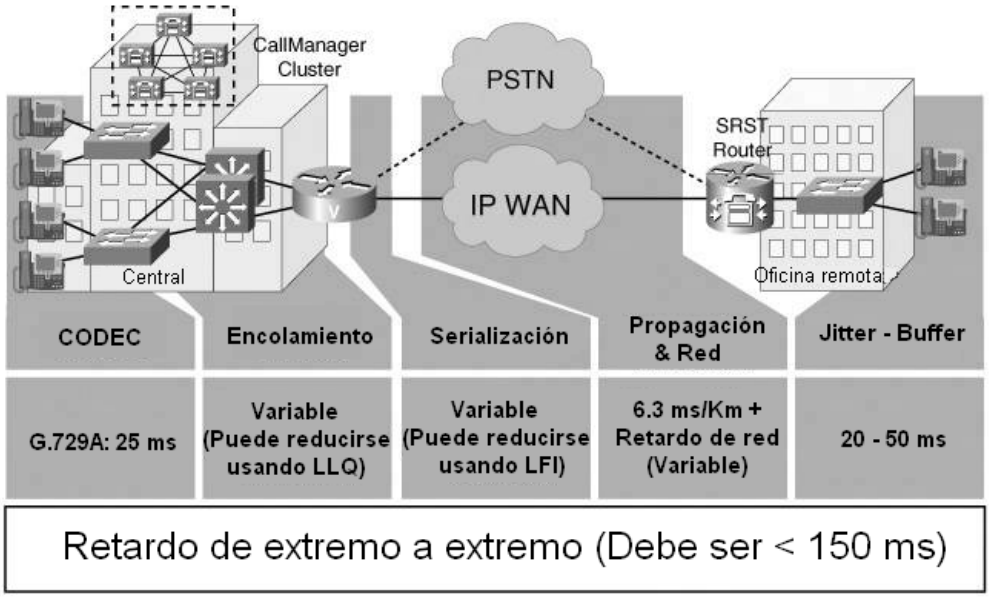

Figura 24. Componentes de retardo de extremo a extremo

El **primer retardo en la comunicación es introducido por el CODEC**. El CODEC toma la muestra de voz, la procesa y crea un paquete de voz. El tiempo que le toma realizar este proceso depende del tipo de CODEC seleccionado.

El **Retardo de encolamiento** es el segundo componente que introducirá retardo en la comunicación. La congestión en la red provoca este encolamiento en los routers. Para reducir el retardo producido por el encolamiento utilizaremos el mecanismo Low Latency Queuing (LLQ, método de encolamiento para VoIP).

El **Retardo de serialización** es el tiempo que toma colocar el paquete en la línea de transmisión y depende de la velocidad del medio. Este valor se define calculando el tiempo que toma en enviar 1 byte en el circuito a la velocidad apropiada. El

siguiente ejemplo ilustra el cálculo del retardo de serialización para un enlace de 64 kbps:

64 Kbps/8 bits = 64000/8bits = 8000 bytes por segundo

1 segundo / 8000 bytes por segundo = 125 microsegundos para transmitir 1 byte.

El **Retardo de propagación** consiste en la cantidad de tiempo que toma transmitir los bits del paquete IP a través del medio de enlace físico. Los factores que influyen son la distancia del circuito entre los routers fuente y destino y el tipo de medio que se utiliza.

Con respecto al **Retardo producido por jitter y el empleo del buffer**, cuando las tramas son transmitidas a través de una red IP, la cantidad de retardo experimentado por cada trama puede diferir debido a que la cantidad de retardo de encolamiento y tiempo de procesamiento puede variar dependiendo del tráfico cargado en la red. Sin embargo el gateway fuente genera tramas de voz a intervalos regulares (es decir, cada 20 ms), y el gateway destino no recibirá tramas de voz en intervalos regulares debido al problema del jitter.

La estrategia para solucionar el problema de jitter es almacenar las tramas recibidas en un buffer tan grande que permita a las tramas más lentas arribar a tiempo para ser ubicadas en la secuencia correcta. Para minimizar el retardo debido al buffering, se emplea un buffer jitter adaptivo. En otras palabras, si la cantidad de jitter en la red es pequeño, el tamaño del buffer será pequeño. Si el jitter se incrementa debido al aumento del tráfico en la red, el tamaño del buffer de destino se incrementará

automáticamente para compensarlo. Por consiguiente, el jitter en la red empeorará la calidad de voz en la magnitud que crece el retardo de extremo a extremo debido al buffer de destino.

Cuando se tiene exceso de jitter en la red y el buffer no puede mantener todos los paquetes, éstos son desechados. Es importante controlar el jitter con una combinación de LLQ y modelamiento del tráfico.

La función de un router es transmitir paquetes tan rápido como sea posible y ubicarlos en el cable. Las capacidades de la red de 2 y 4 Mbps son las velocidades máximas del enlace, sin embargo en el enlace PDH debe considerarse el valor de la tasa de información comprometida (CIR, Committed Information Rate), que es el caudal promedio garantizado que la red se compromete a dar en una conexión durante un intervalo de tiempo definido. Cada router tratará de transmitir a una velocidad mayor a la asignada por el CIR; esto causa congestión en la red; por lo tanto generaría pérdida de paquetes. Es importante entonces cambiar los patrones de tráfico y asegurarnos de que el router considere el valor CIR. En esto consiste el **modelamiento del tráfico**.

Se pondrá atención en la congruencia de las velocidades de los enlaces entre las centrales, de lo contrario se experimentará mayor retardo de los paquetes de voz.

Como conclusión, el modelamiento del tráfico ayudará a no caer en los siguientes problemas:

- Incongruencia de velocidad del enlace
- Sobre-suscripción de sitios remotos al sitio central
- Envío mayor al CIR

Posterior al despliegue de QoS en la infraestructura de WAN, una de los pasos más importantes es el **Aprovisionamiento de ancho de banda de la WAN**. Deberemos asegurarnos que la suma de tráfico de voz, video, control de voz y video y datos no exceda el 75 % del ancho de banda. El 25% restante se utilizará para tráfico de protocolos de enrutamiento.

A continuación, en la Tabla XL se presentan ciertos valores de CODEC y su tasa de muestreo para las consideraciones de ancho de banda. Estos valores consideran el overhead de capa 3.

Tabla XL. Consumo de ancho de banda para voz (sin overhead de capa 2)

CODEC	Tasa de muestreo	Payload en Bytes	Paquetes por Segundo (pps)	BW por Conversación
G.711	20 ms	160	50.0	80.0 kbps
G.711	30 ms	240	33.3	74.7 kbps
G.729a	20 ms	20	50.0	24.0 kbps
G.729a	30 ms	30	33.3	18.7 kbps

Como se muestra en la Tabla XL, el incremento de la tasa de muestreo reduce el ancho de banda requerido, ya que se reduce el overhead del protocolo.

También es necesario considerar overhead de capa 2. La Tabla XLI provee el consumo de BW considerando el overhead de capa 2.

Tabla XLI. Consumo de ancho de banda para voz (con overhead de capa 2)

Codec:Tasa de muestreo	**Ethernet 14 Bytes de Cabecera**	**PPP 6 Bytes de Cabecera**	**MLPPP 10 Bytes de Cabecera**	**Frame Relay 4 Bytes de Cabecera**	**ATM 53-Byte Cells con a 48-Byte de Payload**
G.711 a 50.0 pps Tasa muestreo 20 ms	85.6 kbps	82.4 kbps	84 kbps	81.6 kbps	106 kbps
G.711 a 33.3 pps Tasa muestreo 30 ms	78.4 kbps	76.3 kbps	77.3 kbps	75.7 kbps	84.8 kbps
G.729a a 50.0 pps Tasa muestreo 20 ms	29.6 kbps	26.4 kbps	28.0 kbps	25.6 kbps	42.4 kbps
G.729a a 33.3 pps Tasa muestreo 30 ms	22.4 kbps	20.3 kbps	21.3 kbps	19.7 kbps	28.3 kbps

La Tabla XLI muestra una vez más que el incremento de la tasa de muestreo disminuye el ancho de banda requerido para redes ATM. La tasa de muestreo para los CODECs se modifica en el CallManager al cambiar los siguientes parámetros:

- PreferredG711MillisecondPacketSize (default 20 ms)
- PreferredG723MillisecondPacketSize (default 30 ms)

- PreferredG729MillisecondPacketSize (default 20 ms)

Al modificar estos parámetros afectarán a todos los dispositivos IPT unidos al cluster (agrupación de servidores que operan en conjunto con el CallManager cuando tiene una arquitectura distribuida).

Es importante considerar dos factores cuando se cambia la tasa de muestreo:

- El cambio añade más latencia debido a los retardos de paquetización y serialización.
- Si se pierde un paquete de una muestra de mayor tamaño, se afectará la calidad de voz debido a que se está perdiendo más información.

La **compresión de voz** permite reducir el tamaño en bytes de un paquete IP. Un paquete de voz contiene además de la información útil, información de los protocolos RTP, UDP e IP. La cabecera de un paquete es de 20 bytes, la cabecera UDP es 8 bytes, y la cabecera RTP es 12 bytes, sumando un total de 40 bytes de información de cabecera, es decir el doble del tamaño de la información útil.
Para resolver este problema, existe una técnica de compresión de RTP llamada cRTP (RTP comprimido) utilizado para enlaces de baja velocidad. Con ello se logra reducir la cabecera de 40 bytes a 2 o 4 bytes.

A continuación, en la Tabla XLII se muestran ciertos valores de consumo de BW con cRTP.

Tabla XLII. Consumo de ancho de banda con cRTP

CODEC	ATM 53-Byte Cells con 48-Byte Payload
G.711 a 50.0 pps	85 kbps
G.711 a 33.3 pps	84.0 kbps
G.729a a 50.0 pps	21.2 kbps
G.729a a 33.3 pps	14.1 kbps

Es importante restringir el uso de cRTP en enlaces de baja velocidad. Para enlaces de alta velocidad es mejor no utilizarlo; para evitar saturar al router de procesos extras de compresión y descompresión. En enlaces de alta velocidad, si el tráfico de voz excede más del 30% de la capacidad del enlace, puede habilitarse cRTP para reducir costos.

La Figura 25 resume todas las técnicas discutidas y analizadas hasta el momento en este capítulo para las diferentes capas en la red con el fin de garantizar la entrega de los paquetes en la red.

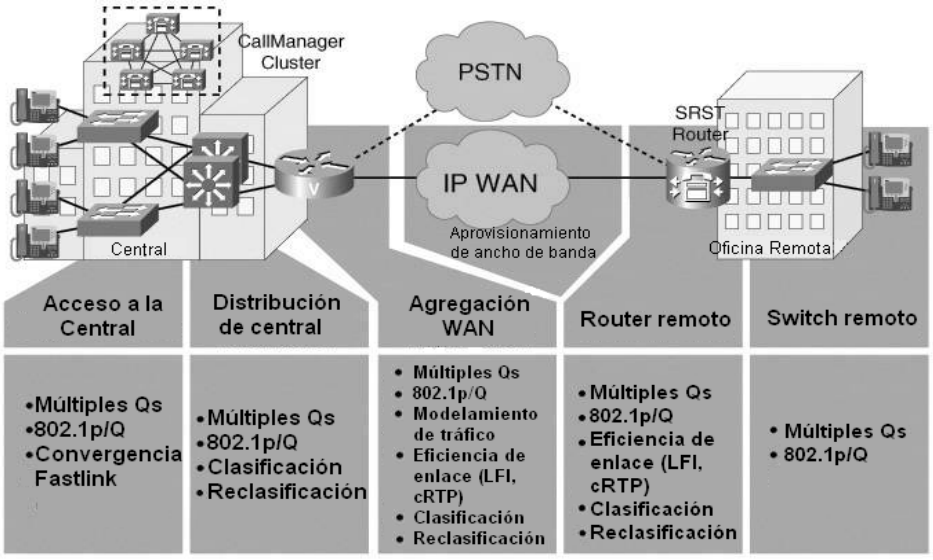

Figura 25. Red IPT con entrega de extremo a extremo garantizada

5.5 Calidad de servicio en la Infraestructura de la LAN

El diseño de QoS en la red consiste en dar un tratamiento preferencial a ciertas aplicaciones sobre otras durante el periodo de congestión. La QoS se configura en la red de acuerdo a las necesidades de cada instancia. En el diseño IPT deberemos dar al tráfico de voz la mayor prioridad, seguido de aplicaciones de video y de datos.

En caso de ser necesario, se dividirán las aplicaciones de datos en algunas clases, debido a que algunos datos podrán ser más críticos que otros.

La calidad de servicio es un mecanismo de punto a punto, y en redes IPT comienza en los teléfonos IP. Algunos teléfonos IP tienen tres puertos de 10/100 Mbps; el empleo de los puertos es el siguiente:

- El puerto 0 se conecta a las aplicaciones de teléfonos IP
- El puerto 1 (llamado el puerto de acceso) se conecta a una PC o cualquier otro dispositivo
- El puerto 2 se conecta al switch de la capa de acceso por donde pasa todo el tráfico desde y hacia los puertos 0 y 1

El tratamiento que se le da a la información en el switch de acceso estará en función del tipo de dato; el tráfico de voz tendrá mayor prioridad que el de video-conferencia; el de video-conferencia tendrá mayor prioridad otro tipo de dato.

La QoS a emplearse permitirá que los paquetes IP en tiempo real optimicen el uso del ancho de banda de la red, garantizando recursos de red suficientes.

A fin de lograr los niveles de calidad de servicio requeridos, haremos uso del campo ToS (Tipo de Servicio) del paquete IP. En la Figura 26 se muestra los diferentes protocolos en la capa 3 que podemos emplear.

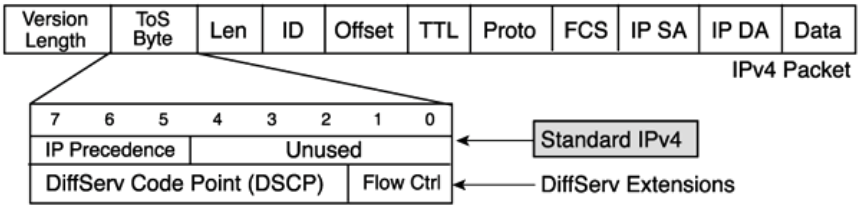

Figura 26. Protocolos de Capa 3 que se emplean en QoS

A continuación en la Tabla XLIII se muestran los valores que deberán ser etiquetados en el Campo ToS de emplearse de DSCP (Punto de Código de Servicios Diferenciados, que permite asignar niveles de servicio) o Prioridad IP.

Tabla XLIII. Valores DSCP y Prioridad IP para ToS

Tipo de servicio	**DSCP**	**Prioridad IP**
Uso RESERVADO	+46	6, 7
Portadora de Voz	46	5
Video Conferencia	34	4
Señalización Llamada	26	3
Datos Prioridad Alta	20	2
Datos Prioridad Media	14	1
Resto de tráfico	0	0

5.6 Servicios de Red

Los servicios de red son importantes para el funcionamiento adecuado de la red. Entre los más importantes tenemos: DHCP, DNS, NTP, directorios y mensajería.

El servicio *DHCP* (Dynamic Host Control Protocol) es importante para proveer escalamiento a la red de telefonía IP. Todas las implementaciones para los teléfonos deberán realizarse a través del DHCP. En la red de datos de las Fuerzas Armadas actualmente no se cuenta con un servicio DHCP, por lo que las direcciones IP han sido asignadas en los equipos de forma manual. Será necesario también realizar una redistribución de las direcciones IP de los dispositivos con los que cuenta la red, debido a que actualmente tales direcciones no están de manera organizada.

El servicio DHCP planificado deberá soportar la opción 150 (Opción suministrada por el DHCP para que un teléfono IP obtenga una dirección IP del CallManager) para implementaciones IPT de Cisco. DHCP utiliza opciones para llevar los parámetros de configuración IP a los clientes. La opción 150 es llamada a la opción TFTP Server Address, que tiene la habilidad de enviar la información del servidor TFTP como una dirección IP.

El servicio *DNS* (Domain Name System) traduce los nombres de dominio a direcciones IP y viceversa. Considerando que se utilizará la opción 150 del servicio

DHCP, utilizaremos el arreglo de direcciones IP para esta opción en lugar de los nombres de las terminales para evitar dependencia en el servidor DNS.

El *servicio de directorio* es utilizado por las empresas para almacenar información relacionada con los empleados tales como ID de e-mail, números de teléfono, localización, ID de usuario, información de autenticación, etc.

La red de las Fuerzas Armadas no cuenta con un servicio de directorio en su infraestructura. El CallManager tiene la capacidad de brindar este servicio mediante el "CallManager Directory Services" (DCD). El CallManager almacena las configuraciones del sistema y de los dispositivos en una base de datos SQL. La información que puede ser almacenada en el DCD es:

- Autenticación de usuario y autorización
- Perfiles de Extensión Mobility (acceso temporal del usuario a la configuración del teléfono IP, permitiendo compartir espacios rotacionales de oficina en lugar de una oficina designada)
- Perfiles de Asistentes Personales
- Directorio personal
- Grabación para marcación por voz
- Discado rápido
- Información de reenvío de todas las llamadas

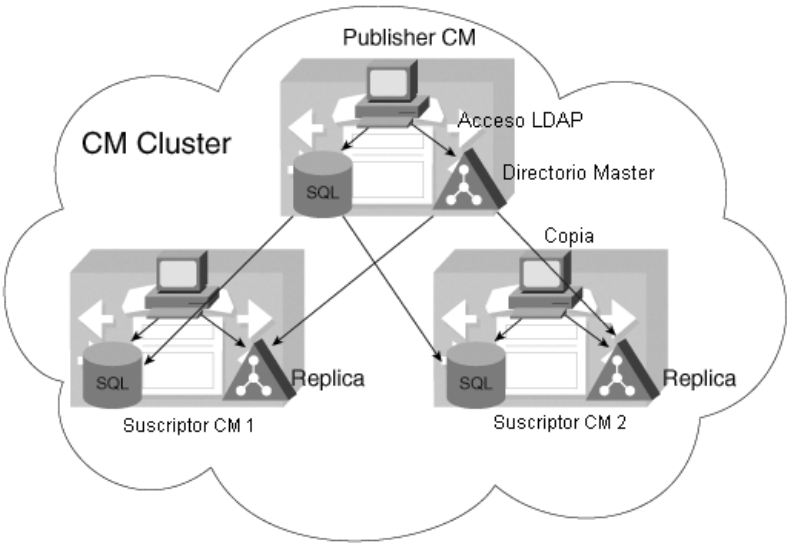

Figura 27. Copia del Directorio DC dentro de un cluster

6. PROPUESTA PARA EL DISEÑO DE LA RED SOLICITADA EN LA RFP

6.1 DISEÑO DE LA INFRAESTRUCTURA DE LA RED

La fase de diseño es el segundo paso que debe realizarse en la metodología del despliegue de una red IPT. Basados en la información recolectada en el cuestionario de la sección 4.6 y de acuerdo al RFP descrito en el capítulo IV, el capítulo VI propone los pasos para la configuración de los dispositivos; basados en la topología de la red para el despliegue de la IPT.

6.1.1 ARQUITECTURA DE PROCESAMIENTO DE LLAMADA

La arquitectura propuesta para la red de datos de las Fuerzas Armadas será el modelo de Procesamiento de Llamada Centralizado, en el cual se desplegarán dos CallManager Cluster Centralizados cuyas aplicaciones estarán localizadas

en los dos nodos más importantes (Quito y Guayaquil) y serán éstos quienes darán asistencia a los dos nodos restantes. Esta arquitectura proveerá de servicio telefónico a los usuarios conectados a los dos nodos de menor demanda; dándoles acceso de forma remota. A continuación se muestra en la Figura 28 la arquitectura de red propuesta en su capa física.

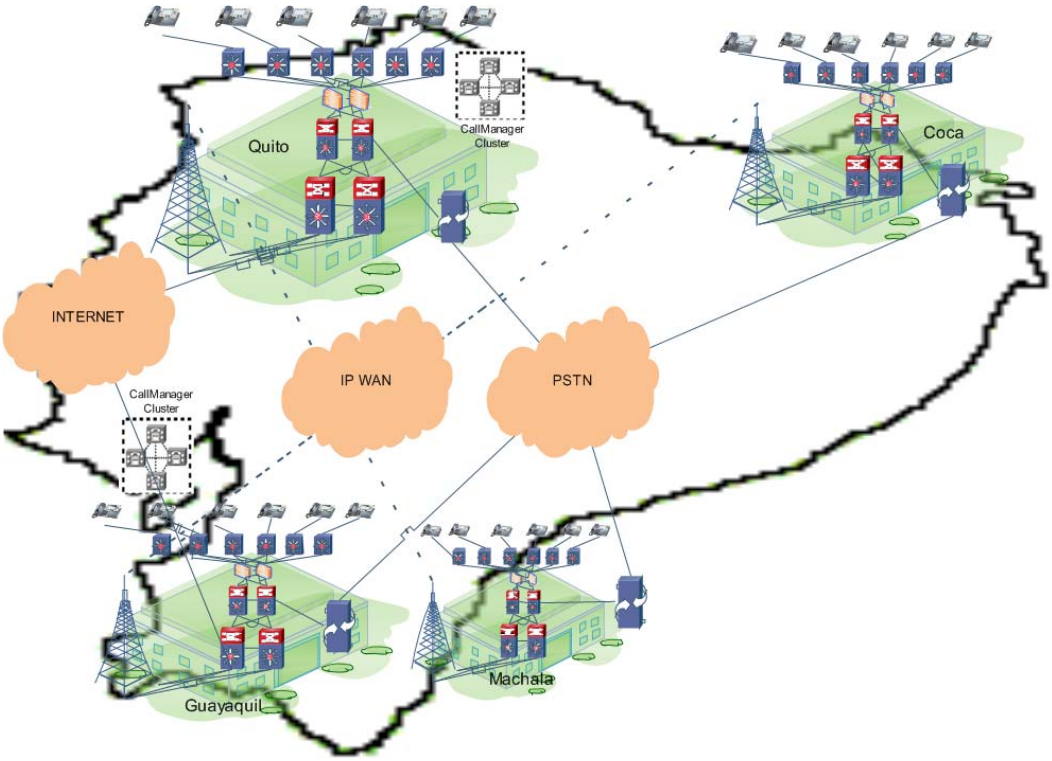

Figura 28. Modelo de arquitectura de red

Como puntos importantes del modelo propuesto debemos señalar:

- La interconexión entre todos los sitios de tipo WAN será mediante el enlace PDH existente.
- El uso de la red conmutada continuará coexistiendo.

- Los teléfonos en los sitios remotos usarán el CallManager Cluster de los sitios centrales para el procesamiento de llamada bajo operaciones normales.

Mediante este diseño hemos brindado redundancia permitiendo soporte de red en caso de desastre, inundación, fuego, derrame de material peligroso o cualquier otro impacto potencial sobre uno de los nodos principales.

6.1.2 SELECCIÓN DE TELÉFONOS IP

La Tabla XLIV muestra el número de usuarios y teléfonos IP planificados para cada nodo. El número de teléfonos IP mostrados incluye teléfonos para usuarios de nivel gerencial, teléfonos requeridos en las salas de conferencia, salas de descanso, salas de espera y áreas comunes.

Tabla XLIV. Número de usuarios y teléfonos IP en cada nodo

Nodo	Número de usuarios	Número de teléfonos IP
Quito	2000	897
Guayaquil	2600	1309
Coca	700	353
Machala	700	353

Existe una gran variedad de teléfonos disponibles en el mercado; pero en función del servicio a brindar a continuación se propone alternativas de

teléfonos en la Tabla XLV. En general, la disposición de los teléfonos IP se realizará de la siguiente manera:

- 7940 y Softphones: Gerentes y asistentes
- 7936: Aplicaciones de videoconferencia
- 7905: Resto de usuarios

Tabla XLV. Cantidad y tipos de teléfonos IP en cada nodo

Nombre del sitio	**Modelo de teléfono**	**Cantidad de teléfonos**
Quito – Ciudadela Militar	7940 Teléfono IP 7936 Videoconferencia 7905 Teléfono IP	100 5 150
Quito – Sector Norte	7940 Teléfono IP 7936 Videoconferencia 7905 Teléfono IP	64 2 576
Guayaquil – Periferia	7940 Teléfono IP 7936 Videoconferencia 7905 Teléfono IP	91 4 636
Guayaquil – Sector Centro	7940 Teléfono IP 7936 Videoconferencia 7905 Teléfono IP	64 2 512
Coca – Unidades militares	7940 Teléfono IP 7936 Videoconferencia 7905 Teléfono IP	32 1 320
Machala – Unidades militares	7940 Teléfono IP 7936 Videoconferencia 7905 Teléfono IP	32 1 320

En los nodos de la red de datos de las Fuerzas Armadas los switches de la capa de acceso son Catalyst 3560, en la versión que no dispone PoE. Todos los teléfonos IP se conectan a los switches de la capa de acceso.

Los switches Catalyst 3560 cuentan con las siguientes características generales:

- Permite el desarrollo de nuevas aplicaciones como Telefonía IP, red de acceso inalámbrico, transmisión de videos de vigilancia, etc.
- Excelente para el desarrollo de redes inteligentes y de nueva generación con avanzadas características de calidad de servicio, listas de control de acceso, ruteo de paquetes IP de manera simple

6.1.3 TAREAS DE DISEÑO DE LA INFRAESTRUCTURA DE LA RED

Con el fin de que la red pueda soportar el tráfico de voz y de datos, la infraestructura deberá tener un adecuado mecanismo de QoS en los siguientes elementos de la red:

- Switches y Routers de las capas de acceso, distribución y núcleo
- Routers de agregación en la WAN
- Routers de sitios remotos

A continuación discutiremos los pasos necesarios para que la red esté lista para soportar trafico IPT.

Para el **Diseño del direccionamiento IP y esquema VLAN** los resultados del cuestionario de la sección 4.6 indican que la red de datos de las Fuerzas Armadas actualmente no posee un esquema de direccionamiento dinámico ni

organizado; por lo tanto, es necesario el diseño del mismo, así como la implementación de VLANs.

Los lineamientos que hemos considerado en esta parte del diseño son:

- Implementación de VLANs separadas para las redes de voz y datos
- Prevención de problemas en la capa 2, no ubicando todos los servidores de procesamiento de llamada y servidores de aplicación en una sola VLAN
- Diseño de un esquema de direccionamiento IP que optimice la información en las rutas (Tablas de Enrutamiento Mejoradas)
- Estandarización en la convención de nombres, en la asignación de los ID de la VLAN y direcciones IP, facilitando la resolución de problemas y la administración de la red

En la Tabla XLVI se muestra el diseño de direccionamiento IP para cada uno de los sitios que conforman la red

Tabla XLVI. VLAN y Asignación de subred para la red de las Fuerzas Armadas

Ubicación	ID de VLAN	Nombre VLAN	Subred VLAN	Descripción
Quito	3	QUITO_SRV1	192.168.3.0/24 GW: 192.168.3.1 HSRP1:192.168.3.2 HSRP2:192.168.3.3	Servidor editor, servidor TFTP, servidor DHCP, servidor de suscriptor 1, IVR 1, y otros servidores del centro de datos como servidores DNS, servidores de correo, etc.
	4	QUITO_SRV2	192.168.4.0/24	VLAN para suscriptor 2, IVR 2, y otros servidores del centro de datos

Ubicación	ID de VLAN	Nombre VLAN	Subred VLAN	Descripción
Quito	5	QUITO_MED	192.168.5.0/24	Para gateways, equipos de conferencia y equipos transcodificadores
	11	QUITO_VOZ1	192.168.11.0/24 GW: 192.168.11.1 HSRP1: 192.168.11.2 HSRP2: 192.168.11.3	Teléfonos IP
	12	QUITO_VOZ2	192.168.12.0/24	Teléfonos IP
	111	QUITO_DAT1	192.168.111.0/24	Usuarios PCs
	112	QUITO_DAT2	192.168.112.0/24	Usuarios PCs
Guayaquil	6	GYE_SRV1	192.168.6.0/24 GW: 192.168.6.1 HSRP1:192.168.6.2 HSRP2:192.168.6.3	Servidor editor de CallManager, suscriptor 1 y Unity 1
	7	GYE _SRV2	192.168.7.0/24	CallManager, suscriptor 2 y Unity 2
	8	GYE _MED	192.168.8.0/24	Para gateways, equipos de conferencia y equipos transcodificadores
	13	GYE _VOZ1	192.168.13.0/24	Teléfonos IP
	14	GYE _VOZ2	192.168.14.0/24	Teléfonos IP
	113	GYE _DAT1	192.168.113.0/24	Usuarios PCs
	114	GYE _DAT2	192.168.114.0/24	Usuarios PCs
Coca	15	COC_VOZ	192.168.15.0/24	Teléfonos IP
	115	COC_DAT	192.168.115.0/24	Usuarios PCs
Machala	16	MAC_VOZ	192.168.16.0/24	Teléfonos IP
	116	MAC_DAT	192.168.116.0/24	Usuarios PCs

Luego de haber realizado el direccionamiento IP y la asignación de las VLANs, el siguiente paso es el **Diseño del servicio de DHCP** que permite identificar el

mecanismo en el que los teléfonos IP reciben la información de direccionamiento; éste permitirá ubicar y administrar el direccionamiento.

En la red de datos de las Fuerzas Armadas, se utilizará un servidor DHCP para el nodo Quito, mientras que para el nodo Guayaquil actuará como DHCP el CallManager Publisher. Los sitios remotos en Coca y Machala obtendrán su direccionamiento IP de los Routers ubicados localmente. En la Tabla XLVII se resume los parámetros a emplearse en el Servidor DHCP de Quito, así como el resto de configuraciones requeridas para cada nodo.

El **Diseño del servicio TFTP** permite almacenar la información de configuración y las cargas binarias para los teléfonos IP y otros terminales IPT. Para el CallManager cluster del nodo Quito, el servidor DHCP también desempeña el rol de servidor TFTP. En el nodo Guayaquil, el servidor CallManager Publisher actúa como servidor TFTP.

Tabla XLVII. Información del servidor de DHCP para la red de datos de las Fuerzas Armadas

Ubicación	**Servidor DHCP**	**Configuración DHCP**
Quito	Nombre: QUIDHCPTFTP IP: 192.168.3.7	**Parámetros comunes** Nombre dominio DNS: COMACO.com Tiempo alquiler: 8 horas Servidor DNS: 192.168.3.20 Opción 150: 192.168.3.8 **Alcance 1** Rango de dirección: 192.168.11.5-254 Máscara: 255.255.255.0 GW: 192.168.11.1 **Alcance 2** Rango de dirección: 192.168.12.5-254 Máscara: 255.255.255.0 GW: 192.168.12.1
Guayaquil	Nombre:GYECCMA-PUB IP: 192.168.6.8	**Parámetros comunes** Nombre dominio DNS: COMACO.com Tiempo alquiler: 8 horas Servidor DNS: 192.168.6.20 Opción 150: 192.168.6.8 **Alcance 1** Rango de dirección: 192.168.13.5-254 Máscara: 255.255.255.0 GW: 192.168.13.1 **Alcance 2** Rango de dirección: 192.168.14.5-254 Máscara: 255.255.255.0 GW: 192.168.14.1
Coca	Router 3845 Nombre: COC-R3750 Dirección IP: 192.168.15.1	**Grupo: IP_PHONE_COC** Rango de dirección: 192.168.15.5-254 Máscara: 255.255.255.0 GW: 192.168.15.1 Opcion 150: 192.168.15.8

Ubicación	Servidor DHCP	Configuración DHCP
Machala	Router 3845 Nombre: MAC-R3750 Dirección IP: 192.168.16.1	**Grupo: IP_PHONE_MAC** Rango de dirección: 192.168.16.5-254 Máscara: 255.255.255.0 GW: 192.168.16.1 Opción 150: 192.168.16.8

En ambos clusters, el servidor DHCP es configurado para que envíe al servidor TFTP la dirección IP (basados en la Opción 150) para los teléfonos y otras terminales.

La **Infraestructura LAN de los sitios centrales** de Quito y Guayaquil de las Fuerzas Armadas se muestra en la Figura 29. Se utilizarán switches Catalyst 3560 en las capas de acceso y Catalyst 6500 en las capas de distribución y de núcleo.

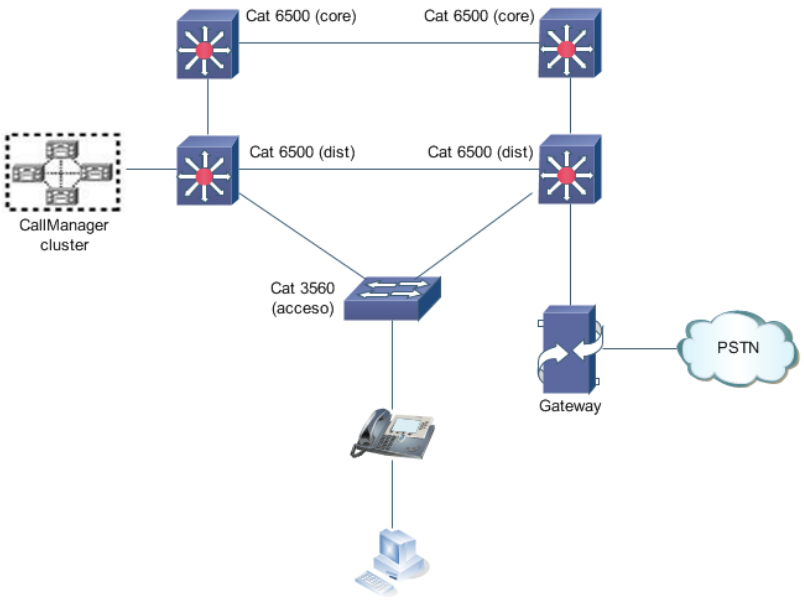

Figura 29. Infraestructura de LAN en los sitios centrales de la red de las Fuerzas Armadas.

Respecto al **Diseño de QoS en la LAN del sitio central**, el empleo de características de QoS en los dispositivos de la red permite asegurar calidad de voz en la red. Estas características deben habilitarse en todo el camino, desde el origen hasta el destino de la llamada.

En una LAN que tiene un gran ancho de banda como la de las Fuerzas Armadas, la QoS se enfocará en el empleo de buffers más pequeños. Por lo tanto, el principal objetivo de la QoS es proteger el tráfico sensible al tiempo (tráfico de voz) de las limitaciones del búfer.

Los lineamientos a seguir al diseñar la QoS en una LAN para redes IPT son:

- Proteger el tráfico de voz, video y cualquier otro tráfico sensible al tiempo contra la pérdida de paquetes causados por buffers o encolamiento
- Proteger contra las configuraciones particulares de envío de paquetes (configuración del byte de ToS para alta prioridad)
- Proveer una frontera de confianza en el borde de LAN para garantizar que se ejecutarán las políticas de QoS en la WAN
- Implementar las configuraciones de QoS de WAN tan preciso como sea posible, considerando ancho de banda y el flujo de tráfico

Las políticas de QoS (que brindan un margen de confianza) verifican la apropiada clasificación de los valores de CoS, ToS y DSCP. Los switches de LAN pueden confiar en los valores de CoS permitiéndoles encolar el tráfico basado en los valores de CoS. El dispositivo LAN pasa los bits de prioridad IP

de capa 3 al dispositivo WAN basado en la clasificación de tráfico recomendada para varios tipos de tráfico, como se muestra en la Tabla XLVIII. En el despliegue de QoS en la red necesitamos identificar el número de clases de servicio que existe en la red y el tipo de tratamiento requerido para cada tipo de tráfico.

Tabla XLVIII. Recomendaciones para Clasificación de tráfico

Tipo de tráfico	**CoS Capa 2**	**Prioridad IP Capa 3**	**DSCP Capa 3**
RTP de voz	5	5	46
Control de voz (SCCP, H.323, MGCP)	3	3	26 24
Dato	0-2	0-2	10-22
Video	4	4	34

Es pertinente mencionar que el estándar de la IETF recomienda que la señalización de paquetes serán marcados con el valor 24 de DSCP en vez del valor 26 de DSCP. Solo ciertas terminales como los Comunicadores IP y los SoftPhone implementan este cambio. Por consiguiente, hasta que esta característica se agregue a todos los productos, deberemos reservar ambos valores para señalización en la red.

Los Switches Catalyst 3560 de la capa de acceso de los nodos no cuentan con PFC, Policy Feature Cards. Es decir, no tendrán la capacidad de clasificar y marcar paquetes IP en la capa 3, sino, se limitarán al valor de CoS de capa 2. Los switches Catalyst 6500 de las capas de distribución y núcleo tienen la

propiedad PFC, por lo que los switches de acceso deberán confiar en los valores ToS dados por aquellos switches, porque cuentan con esa capacidad.

Para la **Configuración de los switches de la capa de acceso** de tipo 3560 se definen a continuación los pasos:

1. Configurar los puertos donde se conectarán los switches, estableciendo la velocidad del puerto, nombre de VLAN de voz y dato
2. Habilitar las capacidades de QoS del switch, ya que están deshabilitados por defecto. Al habilitarlo, todos los puertos se configuran a un estado no confiable
3. Ubicar el tráfico de control de voz en las colas de salida apropiadas. El mecanismo de encolamiento disponible en los switches y routers en la red garantizan menor pérdida y retardo de cierto tipo de tráfico, como la voz. El Catalyst 3560 puede proveer tratamiento preferencial para el tráfico de voz. Cada puerto del Switch tiene una serie de colas de entrada y salida utilizadas como zonas de almacenamiento temporal. El Catalyst 3560 cuenta con dos colas de entrada con tres umbrales de caída y cuatro colas de salida con tres umbrales de caída. Este umbral define el punto en el que el switch puede desechar un paquete en una cola durante una congestión.
4. Asociar los valores de CoS y Prioridad IP a los valores DSCP. Se utiliza CoS – DSCP y Prioridad IP – DSCP para asociar valores CoS y Prioridad IP en los paquetes recibidos a un valor DSCP que el QoS utiliza

internamente para representar la prioridad del tráfico. La Tabla XLIX muestra las relaciones CoS – DSCP y Prioridad IP – DSCP

Tabla XLIX. Relación CoS - DSCP y Prioridad IP - DSCP

CoS/Prioridad IP	0	1	2	3	4	5	6	7
DSCP	0	8	16	26	32	46	48	56

5. Establecer políticas en las interfaces conectadas a los teléfonos IP. Se aplicarán listas de control de acceso como políticas de QoS basado en VLANs. Una Lista de Control de Acceso (ACL) es una tabla que indica a un sistema operativo qué derechos de acceso tiene cada usuario sobre una aplicación o característica particular; así cada objeto tiene un atributo de seguridad que identifica su lista de control de acceso.

   En caso de que un usuario haya cambiado el valor de CoS, ToS y DSCP en su ordenador, la característica del Switch de acceso reasignará este valor a un valor de 0 (aplicación del mejor esfuerzo), y con ello ocurrirá lo siguiente:

   - El switch asignará a las tramas un valor DSCP de 0
   - El borde de confiabilidad se desplaza del Switch al teléfono IP

   Con esto, se califica al puerto del computador como no confiable; aunque no funciona para aplicaciones de SoftPhones; en este caso, se deberá crear un ACL en el switch de acceso para identificar el tráfico RTP de los paquetes UDP, el tráfico de señalización de la PC y otro tipo

de tráfico para marcarlos antes de ser enviados a los Switches de Distribución y Acceso.

6. Restaurar las capacidades de QoS en las interfases conectadas a los switches de distribución y confiar en las etiquetas que vienen de estos

A continuación trataremos la **Configuración de QoS de los switches de la capa de distribución y núcleo**, Switches 6500, en los sitios centrales de Quito y Guayaquil según los siguientes lineamientos:

1. Habilitar QoS en el Switch
2. Ubicar el tráfico de control de voz en la cola apropiada
3. Asociar los valores de CoS y Prioridad IP al valor DSCP
4. Configurar las interfaces que conectan los servidores de CallManager.

   El CallManager configura el valor DSCP a 46 (ToS 5) para tráfico de voz (RTP). Establece también el valor DSCP 26 (ToS 3) para todo el tráfico de control de voz. Sin embargo, el CallManager no utiliza el encapsulamiento de capa 2, IEEE 802.1q, por lo tanto se deberá configurar ACLs que confíen en el valor DSCP y asocien cada ACL al puerto del CallManager
5. Conectar las interfaces a los Gateways, los mismos que soportan valores de prioridad IP y DSCP para tráfico de voz y de control, por lo que debemos usar la ACL para confiar en estos valores
6. Conectar las interfaces de los Switches Catalyst 6500 a los routers WAN apropiadamente configurados, de manera que confíen en el valor DSCP dado por los otros routers y switches de los sitios remotos

7. Configurar los puertos sin uso de los switches de distribución y núcleo a un valor de ToS y CoS de 0

El modelo de procesamiento de llamada elegido es centralizado, por lo que en la **Infraestructura IPT de los sitios remotos,** todos los teléfonos IP conectados en las ramas remotas dependerán, en condiciones normales, del CallManager de los sitios centrales. Ante una falla de WAN, los gateways de voz de los sitios remotos tienen la capacidad de manejar las peticiones de llamadas de los teléfonos en cada sitio respectivo, mediante la característica SRST (Telefonía de Supervivencia de Sitios Remotos, proporciona tolerancia a fallas de la red cuando se pierde conectividad entre un sitio remoto y el CallManager central). La Figura 30 muestra la arquitectura física de los nodos Coca y Machala. Los switches de acceso de los repartos remotos son Catalyst 3560 que conectarán los teléfonos IP respectivos. El router de distribución que utilizaremos es 3845, un router multiservicio, cuyo sistema operativo soporta Acceso de Wan, Gateway de voz, Seguridad, Aplicaciones de discado, QoS, VPN, Firewall, etc.

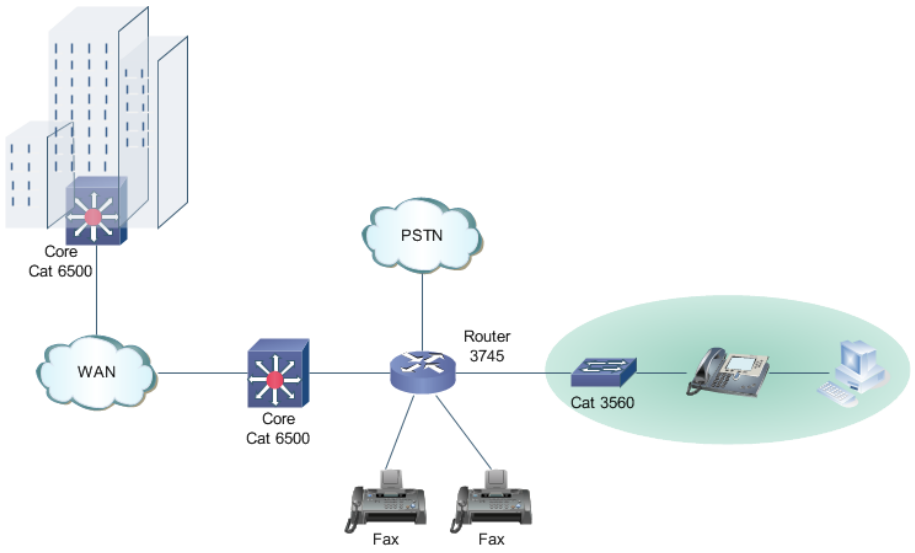

Figura 30. Arquitectura IPT en los sitios remotos

Para el **Diseño de QoS en la LAN de los sitios remotos**, los requerimientos son similares a los de los sitios centrales. La Figura 31 resume las áreas en las que debe enfocarse la configuración de QoS en los sitios remotos.

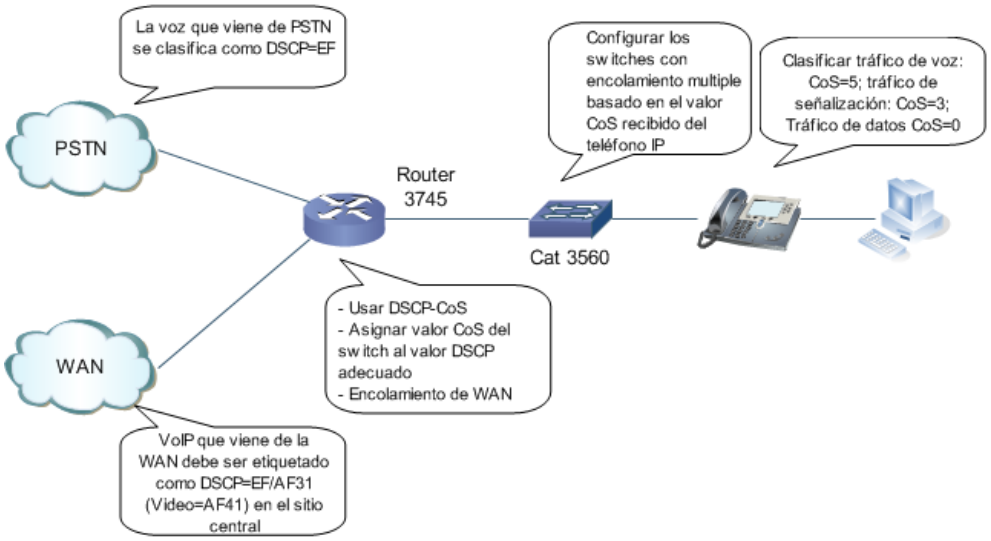

Figura 31. Lineamientos para configuración de QoS en los sitios remotos

En la **Configuración de QoS de los switches LAN de los sitios remotos** podemos decir que se cuenta con switches de acceso Catalyst 3560, los mismos que deben disponer de las siguientes características:

- Estrategia de encolamiento FIFO (first-in, first-out) para las interfases
- Interface del Catalyst 3560 con dos colas de entrada y cuatro colas de salida. La configuración de estas interfaces se indica en la Tabla L, que describe la categorización del tráfico para los paquetes de entrada y de salida para el Catalyst 3560

Tabla L. Categorización del tráfico para el switch Catalyst 3560

	Tráfico VoIP	**Tráfico de control VoIP**	**Tráfico Protocolo de enrutamiento**	**Tráfico STP BPDU**	**Tráfico Video de Tiempo Real**	**Tráfico de otro tipo**	
DSCP	46	24, 26	48	56	34	-	
CoS	5	3	6	7	3	-	
CoS-Cola de entrada	2, 3, 4, 5, 6, 7 (cola 2)					0, 1 (cola 1)	
CoS-Cola de salida	5 (cola 1)	3, 6, 7 (cola 2)			4 (cola 3)	2 (cola 3)	0, 1 (cola 4)

La configuración del Catalyst 3560 para la habilitación de QoS se describe en los siguientes pasos:

1. Habilitación global de QoS en el switch
2. Modificación de la asociación CoS-DSCP por defecto. Los nuevos valores DSCP serán 0 8 16 26 34 46 48 56

3. Modificación de la asociación DSCP-CoS por defecto. Los nuevos valores DSCP serán 0 8 16 26 34 46 48 56
4. Habilitación de encolamiento de prioridad (deshabilitado por defecto) en las interfases del switch que se conectan a los teléfonos IP
5. Ubicación del tráfico CoS 5 en la cola de prioridad y el tráfico CoS 3 en la cola 3. Las etiquetas CoS 6 y CoS 7 son ubicados en la cola 4 y CoS 4 se ubican en la cola 3
6. Habilitación de las características QoS en los puertos del switch que conectan los teléfonos IP (características QoS: valores CoS confiables, creación de VLANs para voz y VLANs para datos, valores en puertos PC no confiables, configuración de los puertos a un estado de reenvío inmediato)
7. Habilitación de las características QoS para uplink. En las ramas remotas, el Catalyst 3560 se conecta directamente a los routers WAN; considerando que los valores DSCP se han configurado correctamente, es posible configurar el puerto uplink que se conecta al router WAN para que confíe en las etiquetas de los paquetes entrantes

La configuración de los switches en los accesos remotos es igual en todos los repartos; pero se tomará en cuenta el cambio del número de identificación de la VLAN para voz y la VLAN para datos.

En la **Configuración del módulo Ethernet para el router 3845** se debe:

1. Incluir las VLAN de voz y datos en la base de datos de VLAN
2. Elegir la interfaz en el router para conectar los teléfonos IP

3. Configurar el formato de encapsulamiento 802.1Q en el puerto; con esto, el router soporta tráfico etiquetado y no etiquetado en el puerto del switch
4. Configurar la VLAN nativa para enviar y recibir tráfico no etiquetado cuando la interfase se encuentra en el modo 802.1Q de enlace. El tráfico que proviene de la PC, específicamente del puerto de datos del teléfono IP, va en esta VLAN nativa
5. Configurar el puerto del switch como un puerto de enlace
6. Configurar la VLAN de voz
7. Configurar el puerto del switch para que pase por encima de la prioridad recibida de un PC o cualquier otro dispositivo
8. Habilitar la característica PortFast en la interfase principal

En cuanto al **Diseño de QoS en la WAN de los sitios remotos**, como ya se conoce, el tráfico VoIP se forma de dos tipos de tráfico:

- Tráfico de voz (RTP) que es la conversación de voz en sí
- Tráfico de control de llamada o señalización que lleva la señalización necesaria para el establecimiento de la llamada, la terminación de la llamada y los mecanismos de control y reporte

El tráfico de control es típicamente tráfico TCP y el de voz es siempre UDP. Estos dos tipos de tráfico deben ser tratados de manera diferente. El tráfico de voz debe ser encolado con las mínimas probabilidades de caída o retardo en la red. El tráfico TCP no necesita ser tan sensible como el UDP ya que este puede ser retransmitido en caso de pérdida de estos paquetes.

Considerando que cada tipo de tráfico necesita diferentes tratamientos, los elementos de la red cuentan con métodos para diferenciar y separar estos flujos de datos. Es por ello necesario la utilización de esquemas que permitirán alcanzar mayor eficiencia en la red, que combinados los conocemos como LLQ.

La Tabla LI muestra la clasificación que se le da a los diferentes tipos de tráfico en los sitios remotos. Como ya se ha mencionado, se debe notar que el tráfico de voz se clasifica con mayor prioridad.

Tabla LI. Clasificación del tráfico en los sitios remotos en valores DSCP

Tipo de tráfico	**Valor DSCP**
Tráfico de Voz (RTP)	EF (46)
Tráfico de control VoIP	AF31 (26)
Tráfico de datos crítico	AF21 (18)

En el diseño de los routers WAN, debemos poner especial atención en las siguientes tareas:

- Asociación DSCP-CoS
- Asociación CoS-DSCP en los routers remotos
- Configuración de encolamiento en interfases WAN

La conexión entre un router y un switch es generalmente un enlace IEEE 802.1Q. Los routers de la WAN deben confiar en los valores DSCP de los paquetes que vienen de la WAN. Este router es responsable de realizar la **asociación DSCP-CoS** antes de que pasen los paquetes a los switches de

capa 2. Este procedimiento permite al switch priorizar el tráfico apropiadamente.

En el diseño, el router WAN del sitio remoto es el 3845 y el switch de acceso es un Catalyst 3560, que es un switch de capa 3, permitiendo confiar en los valores DSCP y sin necesidad de realizar la asociación DSCP-CoS.

La configuración de **asociación CoS-DSCP** en el router WAN 3845 debe realizarse según se indicó en la Tabla LI.

Respecto a la **Configuración de encolamiento en interfases** WAN, en el borde de los routers WAN (router WAN del sitio central y router WAN del sitio remoto), el tráfico de voz necesita ser asignado a un LLQ y el tráfico de control de voz debe tener garantizado el ancho de banda mínimo con mecanismos de CBWFQ.

6.2 DISEÑO DE LA INFRAESTRUCTURA DE PROCESAMIENTO DE LLAMADA Y APLICACIONES

En este capítulo se analizarán las tareas y los procesos que están involucrados en el diseño de la infraestructura de procesamiento de llamada y las aplicaciones de la IPT que requiere la red de datos de las Fuerzas Armadas. Se cubrirán los siguientes temas:

- Diseño de IPT de alto nivel
- Diseño de bajo nivel

- Garantía de la infraestructura IPT

6.2.1 DISEÑO DE IPT DE ALTO NIVEL

Esta sección cubre los aspectos del diseño de alto nivel para el sistema de telefonía IP propuesto por las Fuerzas Armadas.

- Fax y terminales analógicos
- Gateways de voz
- Recursos de media
- Aplicaciones IPT

6.2.1.1 Fax, Terminales Analógicos, Gateways de voz y Aplicaciones IPT

A fin de cubrir los requerimientos de **Fax** de los Routers emplearemos el equipo VG248 y los puertos FXS. El VG248 de Cisco permite conectar teléfonos analógicos, módems y equipos de fax al sistema de CallManager de la IPT vía SCCP (Skinny Client Control Protocol). Cada equipo VG248 cuenta con 48 puertos analógicos FXS para conectarse directamente con los teléfonos analógicos, módems o faxes. El equipo analógico que se conecta al puerto FXS se comporta como si estuviera conectado a una Oficina Central y soportará funcionalidades como llamada en espera, identificador de llamada y transferencia de llamada.

Se desplegará 1 equipo VG248 en Quito y 1 VG248 en Guayaquil. De esta manera, se tendrán 1 x 48 = 48 puertos analógicos en Quito y 1 x 48 = 48 puertos analógicos en Guayaquil.

En lo referente a los **Gateways de voz**, permiten la conexión de la red IPT con una PSTN. A continuación definiremos los módulos de Gateway y los protocolos que se utilizarán para la interfaz IPT – PSTN.

Cada sitio en la red de datos de las Fuerzas Armadas tendrá acceso a la PSTN. En cada nodo, el primer camino hacia la PSTN es el Gateway local. Las llamadas entre dos puntos dentro de la IPT se realizarán preferentemente por la misma red y serán re-enrutadas en caso de una caída del enlace WAN o por falta de ancho de banda disponible para establecer la llamada internamente.

La Tabla LII muestra el hardware utilizado para el acceso a la PSTN y el tipo de señalización PRI usado para el enlace en cada nodo.

Tabla LII. Lista de Hardware para los troncos PSTN y tipo de señalización

Ubicación	Hardware	Tipo de Señalización	Número de enlaces
Quito	WS-SVC-CMM-6E1	E1 PRI ISDN	3
Guayaquil	WS-SVC-CMM-6E1	E1 PRI	3
Coca	NM-HDV-1E1-30E	E1 PRI	1
Machala	NM-HDV-1E1-30E	E1 PRI	1

- WS-SVCCMM-6E1, Modulo tipo Gateway E1, permite conectar una red TDM a una Red IP
- NM-HDV-1E1-30E, High Density Voice Network Module, módulo que combina una interfaz WAN y una interfaz de Voz permitiendo conectividad de voz analógica, voz digital de alta densidad, etc. Cuenta con 5 PVDMs.

Si hablamos de las **Aplicaciones IPT**, mencionaremos los recursos de media, encargados de proveer recursos para conferencia, conversión de codec (transcodificación), Punto Terminal de Media (MTP, software/hardware que permite pasar una trama de una conexión a otra). El MTP puede encontrarse como hardware y software. La transcodificación requiere el uso de DSPs, por lo que consiste en hardware únicamente.

Todos los CallManager en los clústers permiten conferencia y MTP. Es evidente que la habilitación de estos recursos causará un mayor consumo de los recursos del CallManager; por lo que habrá que tomar en consideración estos servicios al momento de analizar la carga en los dispositivos.

La red de las Fuerzas Armadas se desplegará con equipos de hardware para cumplir estas tareas, por lo que se deshabilitará los recursos de media del CallManager para reducir su carga.

Utilizaremos para el diseño de la red IPT un despliegue de recursos centralizado para las peticiones de conferencia y transcodificación. Esta decisión consume un mayor ancho de banda (los paquetes viajan de los sitios remotos al sitio central), el mismo que esta red dispone para todos sus enlaces considerando que se emplea el CODEC G.729a propuesto anteriormente, por lo que esta opción permitirá un ahorro en equipos de hardware adicionales.

Tendremos dos tipos de servicios de conferencia disponibles en el CallManager:

- **Conferencias multipunto espontáneas (Ad-hoc conferencing)** en el que el iniciador de la llamada tiene la facultad de iniciar y controlar la conferencia, siendo el único que puede agregar participantes.
- **Conferencias multipunto programadas (Meet-me conferencing)** donde todos los participantes cuentan con un número de directorio o puente preconfigurado al que pueden marcar para unirse a la conferencia.

Los recursos de transcodificación convierten los datos de un tipo de compresión a otro. En el despliegue de la red IPT de las Fuerzas Armadas se utilizará el CODEC G.729 para las llamadas de voz. El servicio de fax se desplegará con CODEC G.711. En los casos en

que se necesite conversión G.729 a G.711 o viceversa se utilizará un transcodificador basado en hardware.

A continuación se describe el despliegue de los recursos de transcodificación y conferencia en la red de las Fuerzas Armadas:

- En Quito y Guayaquil, el CMM (Communication Media Module) provee los recursos de conferencia y transcodificación mediante un WS-SVC-CMM-ACT (Adaptador de Transcodificador y Conferencia) que cuenta con cuatro DSPs. Cada adaptador de puerto ACT provee 128 canales (32 canales por DSP). Cada CMM tiene máximo cuatro adaptadores ACT por lo que provee un máximo de 512 canales.
- En Coca y Machala, el router 3845 está equipado con el NM-HDV-1E1-30E que provee la capacidad para conferencia únicamente. Los adaptadores de puerto ACT de Quito y los puertos E1 de Guayaquil realizarán las peticiones de transcodificación

Es oportuno señalar que las aplicaciones que se integran al CallManager son:

- Operador Automático (AutoAttendant, AA)
- Centro de Llamadas (Call Center)

La red IPT en despliegue solicita la funcionalidad de un **Operador Automático** de manera que cada llamada pueda tomarse en el

primer timbre, presentar al usuario un menú de opciones y proveer las siguientes opciones:

- Discado por número de extensión
- Discado por nombre
- Transferencia al operador

El operador automático tiene un número propio. Todo abonado externo que llama a este número se comunicará con el operador automático.

La red de datos tendrá un número independiente para llegar a la **Respuesta de Voz Interactiva, IVR;** los usuarios que se comuniquen con este número tendrán las siguientes opciones:

- Transferir al operador automático
- Transferir a un grupo o reparto militar determinado

En lo que respecta al **Centro de Llamadas**, las Fuerzas Armadas ya poseen dicha capacidad pero aplicada a la Infraestructura de Red existente, por lo que al momento de evolucionar en la red se emplearían los recursos existentes.

6.2.2 DISEÑO DE LA RED IPT DE BAJO NIVEL

El CallManager requiere de ciertas configuraciones para brindar requerimientos específicos. En esta sección analizaremos estas para cubrir las funcionalidades solicitadas.

6.2.2.1 Diseño del CallManager Cluster

El CallManager Cluster en Quito, mostrado en la Figura 32, consta de tres servidores; un CallManager Publisher QUICMA-PUB y dos CallManager Subscribers QUICMB-SUB1 y QUICMC-SUB2. Este centro también contará con un servidor, QUITFTPDHCP, que hará funciones TFTP y DHCP; de esta manera se quitará cierta carga al CallManager Publisher.

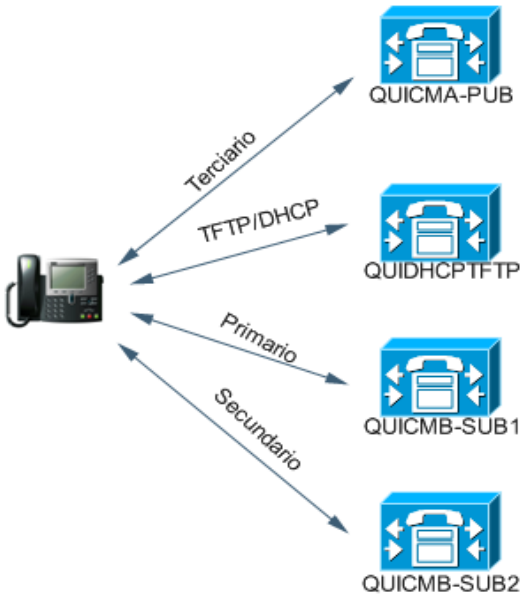

Figura 32. Cluster en Quito

Cada servidor desempeñará las siguientes funciones:

- Servidor QUICMB-SUB1 es el suscriptor primario, en el cual todos los teléfonos IP, Gateways y otros terminales están registrados bajo condiciones normales

- Servidor QUICMC-SUB2 es el suscriptor secundario que realiza funciones de respaldo del suscriptor primario
- Servidor QUICMA-PUB es la base de datos principal de lectura-escritura de la información de configuración del cluster. Permite también mantener la red IPT en servicio cuando ambos servidores suscriptores fallan
- Servidor QUIDHCPTFTP permite en su papel como servidor TFTP la configuración y la carga binaria de los terminales IPT, y como servidor DHCP alquila las direcciones IP para los teléfonos de Quito

La Tabla LIII muestra los nombres de los servidores del CallManager, las direcciones IP y su funcionalidad en el cluster Quito. Estas direcciones están referidas a la Tabla XLVI de la sección 6.1.3 para la asignación de VLANs de la red de las Fuerzas Armadas.

Tabla LIII. Servidores del CallManager Quito

Nombre de Servidor CallManager	Dirección IP de Servidor CallManager	Función	Información de Auto-Registro
QUICMA-PUB	192.168.3.5/24	Editor (Publisher)	Deshabilitado
QUICMB-SUB1	192.168.3.6/24	Suscriptor – procesamiento de llamada primario para todos los dispositivos	Habilitado
QUIDHCPTFTP	192.168.3.7/24	Servidor DHCP, TFTP	No aplica

QUICMC-SUB2	192.168.4.5/24	Suscriptor secundario	Deshabilitado

El CallManager cluster de Guayaquil comprende de dos servidores, como se muestra en la Figura 33. La Tabla LIV describe los nombres de los servidores, dirección IP y funcionalidades de estos servidores.

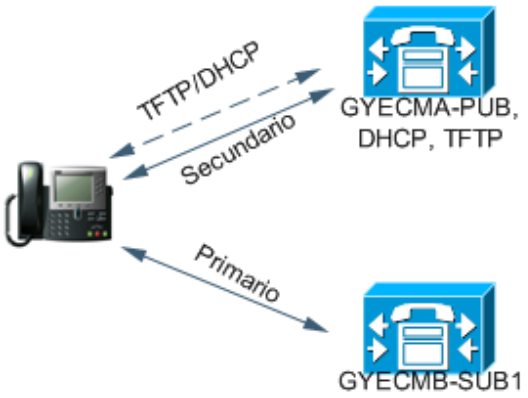

Figura 33. Cluster en Guayaquil

Tabla LIV. Servidores del CallManager Guayaquil

Nombre de Servidor CallManager	Dirección IP de Servidor CallManager	Función	Información de Auto-Registro
GYECMA-PUB	192.168.6.5/24	Editor, servidor TFTP, servidor DHCP	Deshabilitado
GYECMB-SUB1	192.168.7.5/24	Suscriptor - procesamiento de llamada primario para todos los dispositivos	Habilitado

De la Tabla LIII y Tabla LIV se puede observar que el **Auto-Registro** está habilitado únicamente para los servidores primarios; permitiendo a nuevos usuarios telefónicos

registrarse con el servidor de CallManager y obtener un número del directorio especificado en éste. Esta aplicación puede utilizarse en la fase inicial de la implementación para registrar todos los teléfonos IP. Esta función deberá desactivarse después de completado el despliegue de los teléfonos para evitar la conexión posterior de teléfonos no autorizados.

6.2.2.2 Escalabilidad y dimensionamiento del CallManager

El CallManager soporta la conexión de múltiples dispositivos como teléfonos IP, puertos de correo de voz, puertos de Integración de Telefonía por el Computador (CTI), gateways, transcodificadores y recursos de conferencia. Cada dispositivo tiene un propio peso, que consume una determinada cantidad de recursos del servidor durante cada transacción (llamada). Entre estos recursos se menciona la memoria, el procesador y puertos I/O.

El peso de cada dispositivo (métrica) lo calcularemos asumiendo que realiza seis llamadas o menos por hora durante la hora pico o seis llamadas completadas en hora pico BHCC (Busy Hour Call Completion, indica la capacidad de una

central telefónica de *completar* una llamada con el abonado B). La Tabla LV describe los pesos de algunos dispositivos.

Tabla LV. Peso de dispositivos

Tipo de dispositivo	Peso por sesión/Canal de voz	Sesión/DS0 por Dispositivo	Peso total
Teléfono IP	1	1	1
Puertos MGCP analógicos	3	Variable	3 por DS0
Puertos SCCP analógicos	1	Variable	1 por DS0
Punto ruta CTI	2	Variable	Variable
Puerto cliente CTI	2	1	2
Puerto servidor CTI	2	1	2
Control tripartita CTI	3	1	3
Agente de teléfono CTI**¡Error! Marcador no definido.**	6	1	6
Cliente H.323	3	Variable	3 por llamada
Gateway del enlace intercluster	3	Variable	3 por llamada
Gateway H.323	3	Variable	3 por llamada
Puertos gateway T1 del MGCP digital	3	24	72 por T1
Puertos gateway E1 del MGCP digital	3	30	90 por E1
Recurso de transcodificación	3	Variable	3 por sesión
Media Termination Point (MTP) (software)	3	24	72
Recurso de conferencia (hardware)	3	Variable	3 por sesión
Recurso de conferencia (software)	3	24	72

Las Tablas LII y LIII describe el hardware que se despliega en la red IPT. La Tabla XLIV de este capítulo provee la cantidad de teléfonos IP en cada nodo. Con esta información, la Tabla

LVI muestra el peso de los dispositivos que son administrados por el nodo Quito.

Tabla LVI. Cálculos de peso de dispositivos del cluster Quito

Tipo de dispositivo	**Peso por sesión/ Canal de voz [b]**	**Sesiones/DS0s por Dispositivos [c]**	**Total dispositivo [d]**	**Peso total por dispositivo en cluster Quito e = b x c x d**
Teléfono IP	1	1	1250	1250
Puertos SCCP analógicos (1 VG248s, 48 analog ports each)	1	48	3	144
Puertos MGCP analógicos (FXO/FXS)	3	1	10 (FXO + FXS)	30
Punto de ruta CTI	2	1	5	10
Punto cliente CTI	2	1	60	120
Gateway ICT	3	1	1	3
MGCP E1 Digital	3 por DS0	30	4 E1s	360
Recurso de conferencia (hardware)	3 por sesión	96 canales de conferencia por ACT	2 ACTs	576
		36 canales de conferencia en Coca	1	108
Recurso de transcodificación (hardware)	3 por sesión	32 canales de transcodificación ACT	2 ACTs	192
Total				2793

El número total de dispositivos que puede controlar un CallManager varía dependiendo de la plataforma utilizada. El modelo MCS-7835 soporta hasta 5000 unidades de peso. De la Tabla LVI se conoce que el peso del CallManager Quito es

2793, por lo que la plataforma MCS-7835 puede manejar dicha carga y soportar una futura expansión de la red.

La Tabla LVII muestra el cálculo del peso para el cluster Guayaquil.

Tabla LVII. Cálculos de peso de dispositivos del cluster Guayaquil

Tipo de dispositivo	**Peso por sesión/ Canal de voz [b]**	**Sesiones/DS0s por Dispositivos [c]**	**Total dispositivo [d]**	**Peso total por dispositivo en cluster Guayaquil e = b x c x d**
Teléfono IP (incluyendo puerto Unity)	1	1	1662	1662
Puertos SCCP analógicos (1 VG248s, 48 analog ports each)	1	48	3	144
Puertos MGCP analógicos (FXO/FXS)	3	1	10 (FXO + FXS)	30
Punto de ruta CTI	2	1	5	10
Punto cliente CTI	2	1	60	120
Gateway ICT	3	1	1	3
MGCP E1 Digital	3 por DS0	30	4 E1s	360
Recurso de conferencia (hardware)	3 por sesión	96 canales de conferencia por ACT	2 ACTs	576
		36 canales de conferencia en Machala	1	108
Recurso de transcodificación (hardware)	3 por sesión	32 canales de transcodificación ACT	2 ACTs	192
Total				3205

Un cluster de dos MCS-7835 puede manejar la carga de 3205 del cluster Guayaquil.

6.2.2.3 Escalabilidad y Dimensionamiento del Centro de Llamadas y del Operador Automático

El dimensionamiento de un centro de llamada debe considerar los siguientes factores:

- Número de operadores que manejan las llamadas entrantes
- Número de puertos IVR
- Número de gateways PSTN que manejen llamadas que vienen de la PSTN

Para dimensionar estos parámetros se utilizarán dos modelos de tráfico:

- Erlang-B para el dimensionamiento de los puertos IVR y los enlaces de gateway. Este modelo asume lo siguiente:
  - Las llamadas entran aleatoriamente a la red
  - Un porcentaje de las llamadas se bloquea o se pierde en caso de que el enlace esté ocupado. Este porcentaje no se encola

- Erlang-C para el dimensionamiento del número de operadores en el que las llamadas son encoladas antes de ser tomadas por ellos. Este modelo asume lo siguiente:
  - Las llamadas se presentan aleatoriamente a los servidores
  - Los usuarios que se encuentran con todos los agentes ocupados son encolados, no bloqueados

El primer paso para **dimensionar** un centro de llamadas es considerar **el número de operadores**. Con el modelo Erlang-C para este paso se hace uso de los siguientes parámetros:

- Intentos de Llamadas en la Hora Pico (Busy Hour Call Attempts, BHCA), que es el número de llamadas recibidas en la hora pico sin garantizar que la conecta con su destinatario final
- Tiempo Medio de Servicio (Average Handle Time, AHT), que es la duración promedio de una llamada atendida por un operador
- Tiempo Promedio de Trabajo (Average Work Time, AWT), es el tiempo promedio en que un agente toma una llamada después de que el iniciador de la llamada cuelga.
- Meta de nivel de servicio que representa el porcentaje de llamadas a ser contestadas durante un cierto número de segundos

La Tabla LVIII muestra los valores de estos parámetros tomados del historial de reportes del centro de llamadas de las Fuerzas Armadas.

Tabla LVIII. Parámetros para Erlang-C para el dimensionamiento del número de operadores

Parámetro	**Valor**
BHCA	120
AHT	20 segundos
AWT	30 segundos
Meta de nivel de servicio	90 % de las llamadas contestadas en 15 segundos

El cálculo del número de agentes necesarios para atender el centro de llamadas y otros parámetros puede obtenerse a partir de la Calculadora de Centro de Llamadas disponible en http://www.erlang.co.uk/ccc.htm.

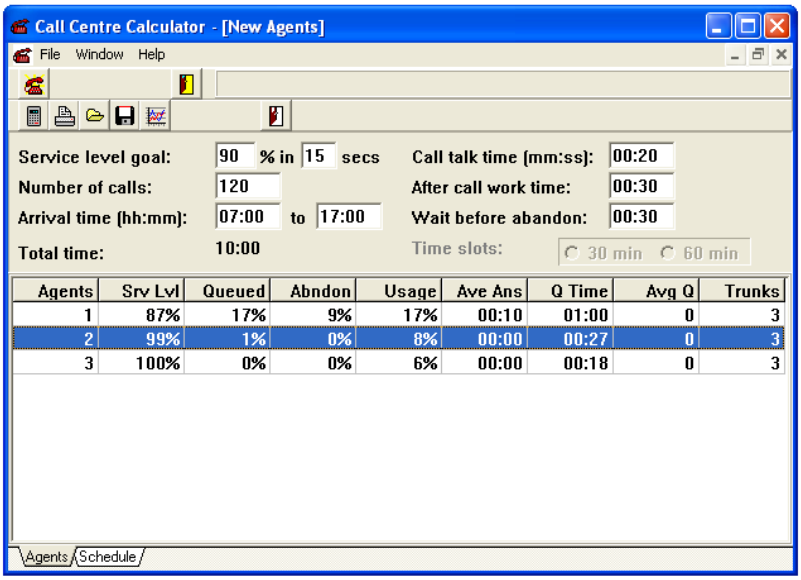

Figura 34. Calculadora de Centro de llamadas

La Figura 34 muestra que el nivel de servicio más cercano al 90% propuesto es de 99% y esto se logra con dos operadores atendiendo el centro de llamadas. Hay otros parámetros que se observan en la Figura 34 y se explican en la Tabla LIX.

Tabla LIX. Resultados de la Calculadora para el Centro de llamadas

Parámetro	**Descripción**	**Valor**
Agents	Número de operadores necesarios para alcanzar la meta de nivel de servicio	2
Srv Lv1	Porcentaje de llamadas que serán contestadas dentro del tiempo de nivel de servicio (15 segundos)	99 %
Queued	Porcentaje de llamadas que deberán ser encoladas por un tiempo antes de ser contestadas	1%
Q Time	Tiempo promedio gastado en la cola para las llamadas que debieron ser encoladas (cuando no hay agentes disponibles)	27 segundos

El parámetro Trunks es el número de enlaces a la PSTN necesarios para el Centro de llamadas. Este número no será tomado en cuenta porque como se dijo anteriormente, para este cálculo se utilizará el modelo Erlang-B.

El segundo paso es **determinar el número de puertos IVR** necesarios para el centro de llamadas. Los puertos CTI o puertos IVR son dispositivos lógicos que manejan los dispositivos telefónicos como puertos utilizados para encolamiento y manejo de sesiones IVR.

El modelo Erlang-B, para el cálculo de los puertos IVR, se basa en los siguientes parámetros:

- BHCA que es el número de llamadas recibidas en una hora pico
- AHT que es la duración promedio de una llamada para aplicaciones autoservicio, que se explican a continuación
    - Periodo de espera inicial cuando el usuario que llama alcanza la red, el mismo que será de 15 segundos.
    - Tiempo de espera en la cola IVR es el número de segundos que el usuario debe esperar en la cola. Debe considerarse también el porcentaje de llamadas encoladas ya que también afecta el número de puertos IVR necesarios. El tiempo de encolamiento promedio se indica en la Tabla LIX, igual a 27 segundos
- Tráfico de hora pico (Busy Hour Traffic, BHT) en Erlangs; cada categoría de AHT es calculada con la siguiente fórmula:

$$BHT = (BHCA \times AHT \text{ segundos}) / 3600$$

Considerando la atención de dos operadores, el valor BHCA en cola será del 1% del total de llamadas, es decir, 120 x 1% = 1,2.

- Bloqueo o grado de servicio es el porcentaje de llamadas que son bloqueadas debido a que no hay puertos IVR disponibles

La Tabla LX muestra los valores BHCA, AHT, BHT y de bloqueo para la red.

Tabla LX. Valores Erlang-B para el dimensionamiento de puertos IVR

Parámetro	Valor
BHCA	BHCA total: 200 BHCA en cola: 1,2
AHT de IVR	Tratamiento de llamada: 15 segundos Tiempo encolamiento promedio: 27 segundos
BHT en Erlangs	BHT1= 120 x 15 / 3600 = 0,5 BHT2= 1,2 x 27 / 3600 = 0,009 Total BHT de IVR = 0.509
Bloqueo	0,1 %

El cálculo de los puertos IVR puede obtenerse mediante la calculadora Erlang-B disponible en http://www.erlang.com/calculator/erlb/.

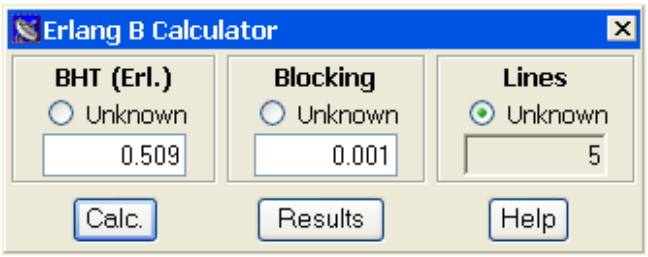

Figura 35. Cálculos de Erlang-B para puertos IVR

La Figura 35 muestra que el número de puertos requeridos para el tratamiento de las llamadas es 5. Este valor es el número mínimo de puertos IVR.

El tercer paso consiste en **determinar el número de enlaces PSTN requeridos para el centro de llamadas (Gateways)**. Se utiliza para este cálculo el modelo Erlang-B, que necesita los siguientes parámetros.

- BHCA es el número de llamadas recibidas en la hora pico
- AHT es el tiempo promedio de una llamada para su tratamiento IVR, encolamiento y tiempo de conversación con el agente. No se incluye el tiempo administrativo de pausa en el cálculo ya que no se utiliza un enlace PSTN
- BHT en Erlangs, donde BHT = (BHCA x AHT segundos) / 3600
- Bloqueo o grado de servicio es el porcentaje de llamadas que encontrarán un tono de ocupado (ya que no hay enlaces disponibles) sin considerarse el BHCA total

Tabla LXI. Valores Erlang-B para el dimensionamiento del enlace PSTN

Parámetro	**Valor**
BHCA	120
AHT	20 segundos
BHT en Erlangs	BHT3 = 120 x 20 / 3600 = 0,66 BHT = IVR BHT + BHT3 = 1,175
Bloqueo	1%

Los valores resultantes del número de enlaces PSTN, basados en el modelo Erlang-B se muestra en la Figura 36, el mismo que indica un valor de 5 líneas.

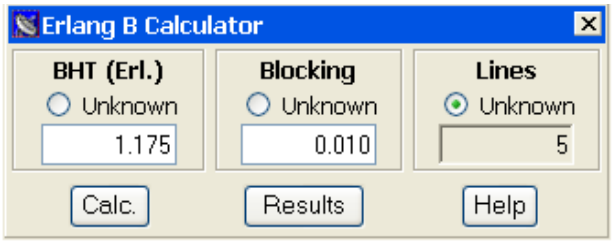

Figura 36. Cálculos Erlang-B para los puertos de enlace PSTN

6.2.2.4 Configuración del Grupo Callmanager

Los servidores de CallManager se enlistan en orden de prioridad. Los teléfonos IP y otras terminales intentan registrarse al primer servidor CallManager especificado en el grupo de CallManager. Si el primer servidor no estuviese disponible, el grupo intenta registrar el terminal a un segundo servidor o en su defecto a un tercer servidor.

Las Tablas LXII y LXIII muestran el nombre del Grupo CallManager y el orden de prioridad de los servidores. La función de Auto-Registro de información para el Grupo CallManager está habilitada, permitiendo así el registro de teléfonos nuevos. Una vez realizado el despliegue y

configuración de todos los terminales en la red, deberá deshabilitarse esta función.

Tabla LXII. Configuración del Grupo CallManager en el cluster Quito

Grupo CallManager	Servidores CallManager	Prioridad	Auto-Registro
QUI-GRP1	QUICMB-SUB1	1	Habilitado
	QUICMC-SUB2	2	Habilitado
	QUICMA-PUB	3	Habilitado

La Tabla LXIII muestra la configuración del Grupo CallManager en el cluster Guayaquil.

Tabla LXIII. Configuración del Grupo CallManager en el cluster Guayaquil

Grupo CallManager	Servidores CallManager	Prioridad	Auto-Registro
GYE-GRP1	GYECMB-SUB1	1	Habilitado
	GYECMA-PUB	2	Habilitado

6.2.2.5 Configuración de la Fecha y Hora del CallManager

Algunos de los grupos Fecha/Hora del CallManager deberán ser configurados de la siguiente manera:

Tabla LXIV. Configuración de Fecha y Hora del CallManager

Grupo CallManager	Zona Horaria	Formato Fecha	Formato Hora
HORAECU	(GMT-05:00) Ecuador	M/D/Y	12-horas

El CallManager sincronizará la fecha y la hora en los teléfonos IP, cada vez que estos sean descolgados y luego colgados.

6.2.2.6 Configuración de Región del CallManager

Las regiones especifican el tipo de códec de voz utilizado para las llamadas entre los dispositivos dentro de una región y entre una región y otra.

Las llamadas dentro de un mismo nodo utilizan G.711 y las llamadas que atraviesan la WAN utilizarán códec G.729.

Las Tablas LXV y LXVI muestran la definición de regiones para los clusters de Quito y Guayaquil respectivamente.

Tabla LXV. Matriz de regiones en el cluster Quito

Regiones	Quito	Coca	Cluster Guayaquil
Quito	G.711	G.729	G.729
Coca	G.729	G.711	G.729
Cluster Guayaquil	G.729	G.729	G.711
FAX	G.711	G.711	G.711

Tabla LXVI. Matriz de regiones en el cluster Guayaquil

Regiones	Guayaquil	Machala	Cluster Quito
Guayaquil	G.711	G.729	G.729
Machala	G.729	G.711	G.729
Cluster Quito	G.729	G.729	G.711
FAX	G.711	G.711	G.711

6.2.2.7 Configuración de Ubicación del CallManager

La ubicación trabaja junto con las regiones para definir las características de un enlace de red. Las regiones definen el tipo de compresión (G.711 o G.729) que es utilizado en el enlace y las ubicaciones definen la cantidad de ancho de banda disponible para el enlace.

Las ubicaciones en el CallManager son utilizadas para implementar CAC (Call Admision Control) en un modelo de procesamiento de llamada centralizado. Antes de permitir una llamada hacia una localidad, el CallManager busca las bases de datos de las ubicaciones para ver si hay algún ancho de banda disponible para esa ubicación. El CallManager rechaza la llamada cuando no hay suficiente ancho de banda para poner una llamada en cierta ubicación.

La Figura 37 describe las regiones, ubicaciones y CODECs utilizados para las llamadas dentro de cada región. Los CODECs utilizados para las llamadas entre regiones y el ancho de banda necesario para las llamadas de voz entre todos los sitios de las Fuerzas Armadas en el cluster Quito. Necesitamos definir una ubicación de CallManager por sitio físico dentro de cada cluster.

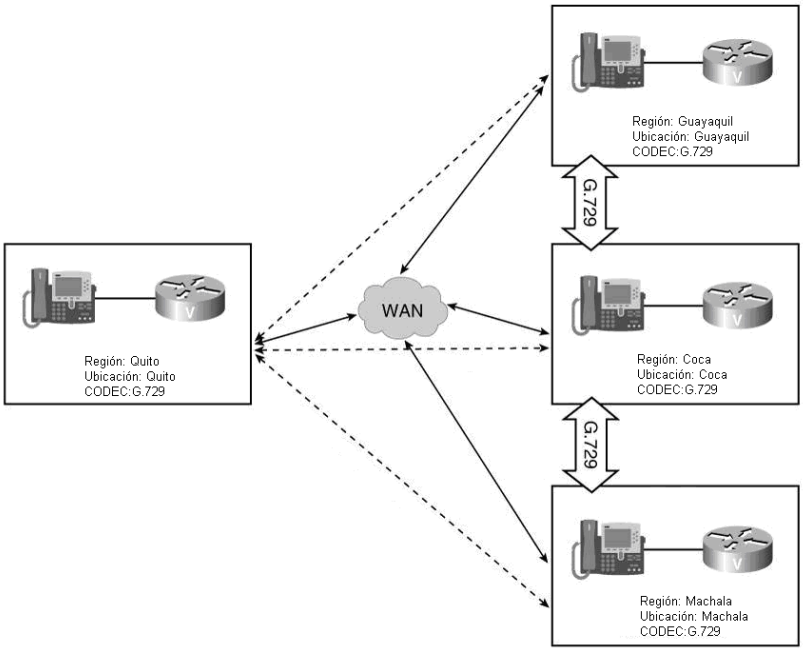

Figura 37. Resumen de las ubicaciones y regiones en las Fuerzas Armadas

Las Tablas LXVII y LXVIII muestra la cantidad de ancho de banda a ser dada para cada ubicación basada en el número máximo de llamadas permitidas entrantes y salientes.

Como indica la Tabla LXVII, permitiremos un máximo de doscientas llamadas en el enlace WAN; la llamada número doscientos uno será rechazada. Considerando el CODEC G.729, se consume 24 kbps por llamada y con un CODEC G.711 una llamada consume 80 kbps. En estos valores no se considera el valor overhead. La utilización de estos valores sacrifica QoS en los enlaces WAN. Un FAX en las ramas tendrá su propia ubicación. Este tipo de llamadas son G.711 que consumen 80 kbps por llamada.

Tabla LXVII. Configuración de la ubicación del CallManager en el cluster Quito

Ubicación	**Máx. llamadas**	**Ancho de banda necesario (Kbps)**	**Ancho de banda disponible (Kbps)**
Guayaquil	200	200 x 24 = 4800	8000
Guayaquil-FAX	5	5 x 80 = 400	
Machala	100	100 x 24 = 2400	4000
Machala-FAX	5	5 x 80 = 400	
Coca	100	100 x 24 = 2400	4000
Coca-FAX	5	5 x 80 = 400	

Tabla LXVIII. Configuración de la ubicación del CallManager en el cluster Guayaquil

Ubicación	**Máx. llamadas**	**Ancho de banda necesario (Kbps)**	**Ancho de banda disponible (Kbps)**
Quito	200	200 x 24 = 4800	8000
Quito-FAX	5	5 x 80 = 400	
Machala	100	100 x 24 = 2400	4000

Machala-FAX	5	5 x 80 = 400	
Coca	100	100 x 24 = 2400	4000
Coca-FAX	5	5 x 80 = 400	

6.2.2.8 Configuración de arreglo de dispositivos

El arreglo de dispositivo es un grupo de parámetros comunes como región, grupo de CallManager, grupo fecha/hora, entre otros que pueden aplicarse a un grupo de dispositivos. Algunos de estos parámetros son configurables en el nivel de dispositivo. Los parámetros que son configurados en el nivel de dispositivo tienen prioridad sobre los parámetros configurados en el nivel de arreglo de dispositivo.

Cada cluster tiene cuatro arreglos de dispositivos. La configuración del arreglo de dispositivos se realiza en el administrador del CallManager. Las Tablas LXIX y LXX listan los nombres de campo y los valores a ingresar para cada uno de los arreglos de dispositivo.

Tabla LXIX. Configuración de arreglo de dispositivo en el cluster Quito

Nombre de arreglo de dispositivo	**Grupo de CallManager**	**Grupo Fecha/Hora**	**Región**	**CSS para auto-registro**
DP-Quito	QU-GRP-1	HORAECU	Quito	CSS-taps
DP-Coca	QU-GRP-1	HORAECU	Coca	CSS-taps
DP-FAX	QU-GRP-1	HORAECU	FAX	CSS-taps

El CSS, Calling Search Space, determina qué destino pueden alcanzar las llamadas entrantes a un Gateway.

Tabla LXX. Configuración de arreglo de dispositivo en el cluster Guayaquil

Nombre de arreglo de dispositivo	**Grupo de CallManager**	**Grupo Fecha/Hora**	**Región**	**CSS para auto-registro**
DP-Guayaquil	GYE-GRP-1	HORAECU	Guayaquil	CSS-taps
DP-Coca	GYE-GRP-1	HORAECU	Machala	CSS-taps
DP-FAX	GYE-GRP-1	HORAECU	FAX	CSS-taps

El diseño del CSS se explica más adelante. Mientras tanto, describimos que los teléfonos auto-registrados hacen lo siguiente:

- Obtiene el CSS especificado del Espacio de búsqueda de llamadas.
- Obtiene el número de directorio y la información de partición.

6.2.2.9 Configuración de Recursos de Media

Los recursos de media consisten en los recursos de conferencia, transcodificación y MTP. En esta sección definiremos el diseño de estos recursos para la red de datos de las Fuerzas Armadas.

Los recursos de **conferencia** se encuentran disponibles en los nodos principales Quito, Guayaquil, Coca y Machala únicamente. En esta sección se analizarán los pasos para la configuración en estos sitios.

En lo referente a **Quito**, el puerto adaptador para media (ACT) del CMM, brindará los recursos de conferencia contando con cuatro DSPs. Estos se particionarán en dos grupos de recursos:

- **Grupo de conferencia:** Se asignará tres DSPs: 3 x 32 = 96 canales
- **Grupo de transcodificación:** Se asignará un DSP: 1 x 32 = 32 canales

Los pasos para la configuración del módulo ACT son:

1. Añadir el Puente de Conferencia en el administrador del CallManager.

El puente de conferencia del CallManager es una aplicación de software o hardware que permite los dos métodos de conferencia: Conferencia Multipunto Espontánea y Conferencia Multipunto Programada. Cada puente de conferencia puede hospedar conferencias múltiples simultáneamente.

Tabla LXXI. Adaptador de puerto del ACT Quito en las configuraciones del CMM

Parámetro	**Valor**
Tipo de Puente de Conferencia	Puente de Conferencia del Cisco IOS
Nombre del Puente de Conferencia	PCF001122334455 001122334455 es la dirección MAC de la interfaz Ethernet asociada al módulo ACT
Descripción	Cat6k-QU-1 CMM ACT Media Card (slot 3)
Arreglo de dispositivo	DP-Quito
Ubicación	<Ninguno>

NOTA: En las Tablas LXXI y LXXIII, la ubicación del puente de conferencia es <Ninguno> porque los recursos se encuentran en los sitios centrales

2. Configurar el CMM desde el CLI (Command Line Interface)

Para **Coca**, el módulo NM-HDV-1E1-30E provee los recursos de conferencia. Este módulo es desplegado con cinco PVDMs (Módulo de Datos de Voz en Paquetes) y cada PVDM tiene tres DSPs. El número de llamadas que es capaz de establecer depende del CODEC utilizado.

El circuito E1-PRI de la PSTN termina en el NM-HDV-1E1-30E. El módulo DSP convierte la información de voz recibida de la PSTN a formato de paquete IP. Se requieren tres

PVDMs para el circuito E1, determinados por el siguiente cálculo:

Bajo codec G.729 y G.711, un DSP puede proveer cuatro canales, por lo que

3 PVDM x (3 DSP x 4 canales por DSP) = 36 canales

De los 36 canales, 32 canales se tomarán para el circuito E1.

Los cuatro canales restantes, se asignarán junto a los dos PVDMs restantes la función de videoconferencia. Cada DSP tiene capacidad para manejar una conferencia con capacidad de hasta seis participantes. Con dos PVDMs más 4 canales, Coca podrá soportar hasta 42 sesiones de videoconferencia.

La configuración de la partición DSP requiere los siguientes procedimientos:

1. Añadir el puente de conferencia (desde el CallManager)

Tabla LXXII. Configuración del Puente de Conferencia para el NM-HDV de Coca

Parámetro	**Valor**
Tipo de Puente de Conferencia	Puente de Conferencia del Cisco IOS
Nombre del Puente de Conferencia	PCF00AABBCCDDEE 00AABBCCDDEE es la dirección MAC de la interfaz SCCP de los routers
Descripción	Coca 3845 NM-HDV-1E1-30E
Arreglo de dispositivo	DP-Coca
Ubicación	Coca

2. Configurar el módulo NM-HDV-1E1-30E en el router 3845 desde el CLI

   La configuración del puente de conferencia en Machala es idéntica al de Coca.

   En **Guayaquil**, la tarjeta WS-SVC-CMM-6E1del Catalyst 6500 será el recurso DSP usado para conferencia. De acuerdo a la Tabla LII, el switch en Guayaquil cuenta con 3 troncos E1s que conectan a la PSTN para enrutar las llamadas entrantes y salientes. Desplegaremos dos módulos WS-SVC-CMM-6E1en dos Catalyst 6500 para lograr redundancia. Este módulo tiene seis puertos E1. Cada puerto puede ser configurado como recursos de conferencia, transcodificación o MTP.

   Es muy importante considerar que en cada módulo E1, el puerto 3 está dado en el CallManager como un recurso de conferencia. Además de configurar este equipo en el CallManager, debe configurarse el Sistema Operativo del Catalyst para ubicar este puerto en la VLAN correcta y habilitar el DHCP.

   Cada puerto del WS-SVC-CMM-6E1 puede controlar 32 participantes mediante G.711 con un máximo de 6

participantes por conferencia. En G.729, cada puerto puede manejar únicamente 24 participantes.

La asignación de la tarjeta WS-SVC-CMM-6E1 como puente de conferencia se realiza desde el administrador del CallManager, y se configura con la siguiente información.

Tabla LXXIII. Configuración del Puente de Conferencia para Guayaquil

Parámetro	**Valor**
Tipo de Puente de Conferencia	Hardware de Puente de Conferencia
Nombre del Puente de Conferencia	PCF00EEDDCCBBA9
Descripción	Cat6k-GY-1 CMM ACT Media Card (slot 3)
Arreglo de dispositivo	DP-Guayaquil
Ubicación	<Ninguno>

Las aplicaciones de **transcodificación** son necesarias en un despliegue con CODEC combinado, de lo contrario la red no podrá funcionar. Los dispositivos transcodificadores se desplegarán en los sitios centrales.

Para los recursos de transcodificación en **Quito y Guayaquil**, se utilizará para cada sitio, un DSP del módulo ACT permitiendo manejar 32 canales. Cada sesión utiliza 2 canales, por lo que el número total de los recursos de transcodificación es 16.

La configuración de los módulos ACT para transcodificación sigue los siguientes pasos:

1. Añadir el transcodificador entre los recursos del CallManager
2. Configurar el CMM desde el CLI

Cada sitio dentro de los clusters Quito y Guayaquil cuenta con un **Gateway** para el acceso a la PSTN. Cada gateway se despliega para diferentes propósitos. Las Tablas LXXIV y LXXV muestran las funciones de cada gateway en ambos clusters y los protocolos de señalización utilizados para la comunicación con el CallManager.

Se despliega un **Gatekeeper** centralizado para proveer enrutamiento de llamadas y CAC entre Quito y Guayaquil. Las llamadas entre los dos nodos se realizan a través de la WAN, pero en caso de falla de la WAN o ancho de banda insuficiente, las llamadas serán enrutadas al gateway PSTN del sitio central.

Debe realizarse configuración del gateway desde el administrador del CallManager, indicando el tipo de gateway y el protocolo de señalización.

Tabla LXXIV. Gateways de voz del cluster Quito - Funcionalidades y Señalización

Ubicación	Nombre del Terminal	Función	Señalización
Quito	S1/DS1-0@QU-CMM1 S1/DS1-1@QU-CMM1 S1/DS1-0@QU-CMM2 S1/DS1-1@QU-CMM2	Acceso a la PSTN para usuarios Quito Acceso a la PSTN para usuarios Coca	MGCP Ubicación:Quito MRGL:MRGL_QU
	Gatekeeper	Llamadas intercluster	ICT
Coca	S1/DS1-0@R3845-COC	Acceso a la PSTN para usuarios Coca	MGCP con H.323 Ubicación:Coca MRGL:MRGL_CO
	AALN/S2/SU0/0@R3845-COC AALN/S2/SU0/1@R3845-COC	Faxes	

El ICT (Intercluster Trunk) es un mecanismo que permite enviar datos que no tienen formato H.323 en un túnel que trabaja con H.323.

La nomenclatura S1/DS1-0@QU-CMM1 representa el Terminal digital MGCP para el controlador E1 1/0. QU-CMM1 es el campo del nombre de dominio al configurarse el CMM. La convención del nombre indica que este DS1 está ubicado en el CMM1, del switch Catalyst 6500 localizado en Quito. Por otra parte, S1/DS1-1@QU-CMM1 representa el Terminal digital MGCP para los controladores E1 1/1 y AALN/S2/SU0/0@R3845-COC representa el Terminal analógico MGCP para el puerto análogo 2/0/0. S2/SU0/0 representa el puerto análogo 2/0/0 ubicado en el NM-HDV-

1E1-30E del router 3845. @R3845-COC indica que el router 3845 se ubica en Coca.

Tabla LXXV. Gateways de voz del cluster Guayaquil - Funcionalidades y Señalización

Ubicación	Nombre del Terminal	Función	Señalización
Guayaquil	S1/DS1-0@GY-CMM1 S1/DS1-1@GY-CMM1 S1/DS1-0@GY-CMM2 S1/DS1-1@GY-CMM2	Acceso a la PSTN para Guayaquil Acceso a la PSTN para Machala	Ubicación: Guayaquil MRGL:MRGL_GYE
	Gatekeeper	Llamadas Intercluster	ICT
Machala	S1/DS1-0@R3845-MAC	Acceso a la PSTN para Machala	MGCP con H.323
	AALN/S2/SU0/0@R3845-MAC AALN/S2/SU0/1@R3845-MAC	Faxes	

6.2.3 ARQUITECTURA DEL PLAN DE DISCADO

El diseño de la red de las Fuerzas Armadas comprende dos CallManager clusters. La arquitectura del plan de discado se presenta en las Tablas LXXVI a XC y cubre todos los aspectos del plan de discado para el cluster Quito.

El plan de discado del CallManager manejará un tipo de llamada:

- Llamadas internas a los teléfonos IP y otros dispositivos registrados al CallManager cluster

El plan de discado para llamadas internas registradas con el CallManager es simple. Previo al diseño del plan de discado, se debe diseñar el **plan de numeración**, que debe tener la siguiente información:

- La longitud de extensión de los números de teléfono utilizados internamente

El plan de numeración utilizará 5 dígitos para cada sitio. Ningún sitio tendrá números de marcación directa. La Tabla LXXVI presenta el plan de numeración para cada sitio de la red.

Tabla LXXVI. Plan de Numeración para la red de las Fuerzas Armadas.

Nombre del sitio	**Rango del directorio**
Quito	50000 – 51999
Guayaquil	52000 – 53999
Coca	54000 – 55999
Machala	56000 – 57999

6.2.3.1 Características para el Enrutamiento de Llamada

Identificaremos los tipos de llamadas en la red y los requerimientos de enrutamiento de llamada. El cluster Quito tiene tres tipos de llamadas:

- Llamadas internas que se originan del teléfono IP de un sitio hacia otro teléfono IP del sitio interno.

- Llamadas externas, hacia números de teléfono externos que no son parte del plan de numeración del CallManager de la red

Con respecto al nodo Quito, el enrutamiento tendrá los siguientes lineamientos:

- Las llamadas externas (locales, larga distancia, internacional) utilizan los troncos de la PSTN
- Las llamadas de emergencia utilizan los troncos de la PSTN en Quito
- Las llamadas externas que entran al nodo Quito son enviadas a una aplicación de operador automático

Con respecto al nodo Coca, el enrutamiento tendrá los siguientes lineamientos:

- Las llamadas externas utilizan la PSTN de Coca como primera preferencia y la PSTN de Quito como respaldo
- Las llamadas de emergencia utilizan los troncos de la PSTN en Coca
- Las llamadas externas entrantes a Coca son enviadas al operador automático en Quito

Las llamadas entre los clusters Quito y Guayaquil utilizarán la WAN IP utilizando ICT preferentemente o en su defecto el tronco PSTN

El **plan de enrutamiento** determina los aspectos de manejo de llamada. Muchos elementos, como los que se muestra en la Figura 38, define el plan de ruta en el CallManager. A continuación se describe brevemente estos elementos:

- Modelo de rutas (Route Pattern) identifica diferentes grupos de números telefónicos. Por ejemplo, un modelo de ruta de 50XXX relaciona los dígitos desde 50000 hasta 50999
- Lista de rutas (Route Lists), es una lista ordenada de grupos de rutas que provee los múltiples caminos para enrutar las llamadas. Se asocia un modelo de ruta con una lista de rutas. Cuando un número marcado coincide con un modelo de ruta, el CallManager enruta la llamada por los grupos de ruta especificados en la lista
- Grupo de ruta (Route Group), es una lista ordenada de dispositivos/gateways que pueden enrutar una llamada a diferentes destinos. El grupo de ruta puede dirigir todas las llamadas al dispositivo principal y luego usar los dispositivos secundarios cuando el principal no estuviese disponible. Una o más listas de ruta pueden apuntar a un mismo grupo de ruta. Ya que un gateway puede ser asignado solo a un grupo de ruta, asignaremos cada gateway a un grupo de ruta porque manejará diferentes modelos de ruta

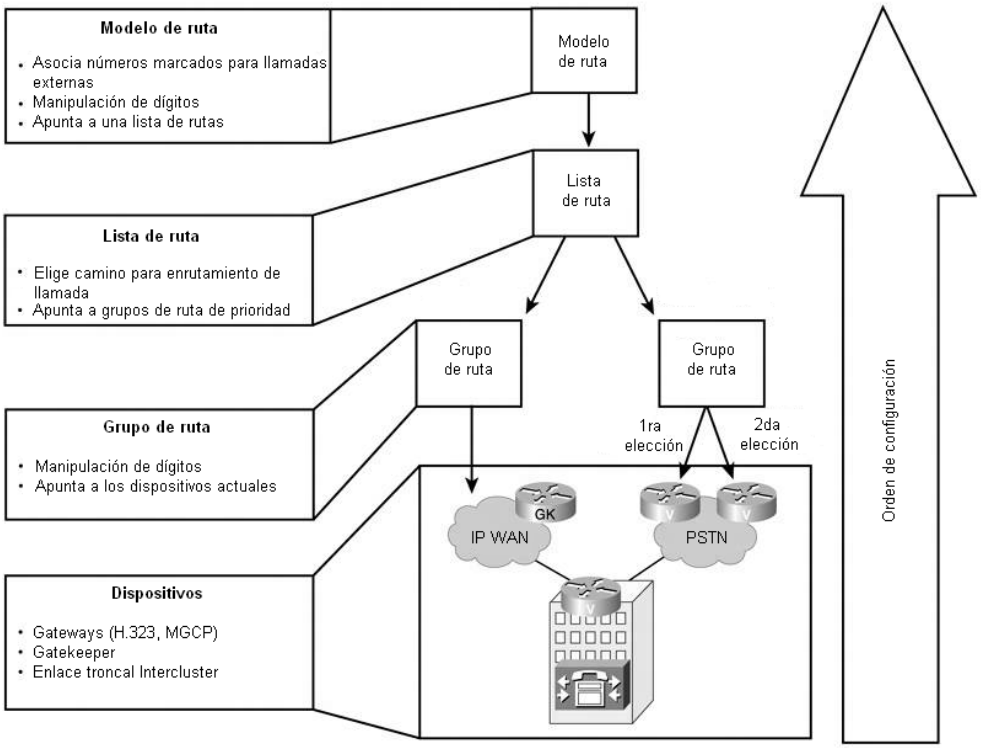

Figura 38. Elementos de un plan jerárquico de rutas en el CallManager

Como se observa en la Figura 38, el orden de configuración para los elementos del plan de ruta es desde la base a la cima, lo que significa que los dispositivos y gateways son configurados primero, seguidos del grupo de ruta, lista de ruta y modelo de rutas.

Luego de identificar los caminos de enrutamiento de llamada, el siguiente paso es el **diseño de particiones**. Una partición es un grupo de dispositivos con características de accesibilidad similares. Las entidades que podemos ubicar en las particiones son modelos de ruta y números de directorio de teléfonos IP, puntos de ruta CTI,

puertos CTI, entre otros. Los modelos de ruta pueden corresponder a destinos internos o externos de la PSTN.

Los criterios empleados para establecer las particiones son las siguientes:

- Números internos y puertos CTI
- Particiones especiales requeridas por aplicaciones específicas
- Números de emergencia por sitio
- Llamadas locales por sitio
- Llamadas de larga distancia por sitio
- Llamadas internacionales por sitio

Ya que cada sitio tiene gateways locales que se conectan a la PSTN, necesitamos definir el mismo modelo de ruta para cada sitio. Los criterios mencionados tienen modelos de ruta separados que deben ser incluidos en el CSS de los teléfonos IP.

La Tabla LXXVII provee las particiones a crearse en la red de las Fuerzas Armadas para el cluster Quito en el plan de discado.

Tabla LXXVII. Particiones en el cluster Quito

Nombre de partición	**Descripción**
P-Interna	Contiene todos los teléfonos IP, faxes, puertos CTI, puntos de enrutamiento CTI
P-Manager-Interna	Contiene todos los números de directorio de gerentes, necesarios para la implementación de IPMA
P-IPMA	Contiene los puntos de ruta CTI de IPMA
P-Emergencia-QU	Llamada a número de emergencia de Quito
P-Emergencia-CO	Llamada a número de emergencia en Coca
P-Local-QU	Contiene los códigos de área para llamadas locales en Quito
P-Local-CO	Contiene los códigos de área para llamadas locales en Coca
P-LD-QU	Contiene los códigos de área para llamadas de larga distancia en Quito
P-LD-CO	Contiene los códigos de área para llamadas de larga distancia en Coca
P-INT-QU	Contiene los códigos de área para llamadas internacionales en Quito
P-INT-CO	Contiene los códigos de área para llamadas internacionales en Coca
P-Block	Bloqueo de números, de ser necesario
P-Block-Local	Bloqueo de Llamadas locales
P-Block-LD	Bloqueo de Llamadas de larga distancia
P-Block-INT	Bloqueo de Llamadas internacionales
P-LD-AAR-CO	AAR de larga distancia para Coca
P-INT-AAR-CO	AAR internacional para Coca
P-Autoregphone	Partición para los teléfonos autoregistrados

- IPMA, IP Manager Assistant, aplicación que ofrece capacidad de encaminamiento de llamadas y otras funciones que ayudan a jefes y secretarias a manejar las llamadas eficientemente.
- AAR, Automatic Alternate Routing es una función que dirige las llamadas a rutas alternas cuando las instalaciones no están disponibles

Coca tiene sus propias particiones aún cuando se utilizan los troncos PSTN de Quito para enrutar llamadas locales y de larga distancia que se realizan desde Coca. Esto es requerido ya que las listas de ruta asignan las llamadas por distintas rutas, dependiendo del origen de la llamada.

CSS es una lista ordenada de particiones que un usuario telefónico busca antes de ser permitido realizar una llamada. El CallManager utiliza el CSS para definir los niveles de CoR (Class of Restriction). Los CSSs son asignados a dispositivos que pueden iniciar llamadas, entre ellos, teléfonos IP, softphones y gateways. Las restricciones de llamada son simples de fijar ya que los usuarios pueden marcar únicamente las particiones en la que ellos están asignados.

La Tabla LXXVIII explica los niveles de servicio CoR disponibles en el CallManager.

Tabla LXXVIII. Clases de restricción

Nivel de servicio	**Permite llamadas a**
1(Teléfonos de recepción)	Todos los teléfonos; números de emergencia y otros servicios, llamadas locales, llamadas sin costo, correo de voz, acceso a otros sitios
2(Teléfonos de personal)	Acceso de nivel 1; más llamadas de larga distancia
3(Teléfonos de gerencia)	Acceso de nivel 2; más llamadas internacionales

La Tabla LXXIX describe los niveles de CoR de la red de las Fuerzas Armadas.

Tabla LXXIX. Niveles de CoR en la red de Fuerzas Armadas.

Nivel de CoR	**Llamadas permitidas por usuario**	**Usuarios que requieren CoR**
1 (por defecto)	Llamadas a todos los teléfonos IP, 911	Teléfonos en lobby
2 (por defecto + local)	Acceso de nivel 1 y llamadas locales	Teléfonos para salas de estar
3 (por defecto + local + LD)	Acceso de nivel 2 y llamadas de larga distancia	Teléfonos para todos los empleados y conferencia
4 (Sin restricción)	Acceso de nivel 3 y llamadas internacionales	Teléfonos para el nivel gerencial

En el CallManager puede asignarse para un teléfono IP el CSS en dos niveles:

- Nivel de línea (nivel de número de directorio)
- Nivel de dispositivo (en el teléfono IP)

La Figura 39 muestra ambos niveles de CSS

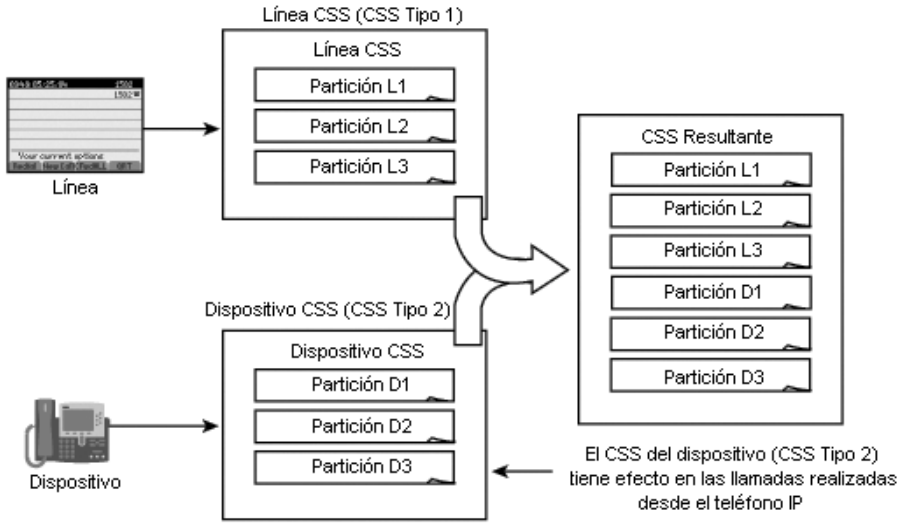

Figura 39. CSS combinado en un teléfono IP

Utilizaremos la combinación de los dos niveles para definir el CoR de la red. Para ello precisamos tres tipos de CSSs:

- **CSS Tipo 1,** atribuido al nivel de línea que le provee a la línea cierto CoS. Es necesario un CSS tipo 1 para cada tipo de CoR requerido
- **CSS Tipo 2,** atribuido al nivel de dispositivo que brinda a un dispositivo el acceso a recursos locales para que alcance la PSTN. Es necesario un CSS Tipo 2 para cada sitio remoto
- **CSS Tipo 3,** es un tipo general que se asigna a recursos tales como puertos CTI y reenvío de llamada en el nivel de línea

La Tabla LXXX señala la lista de CSSs a ser provistas e incluye una breve descripción para el cluster Quito.

Tabla LXXX. CSS en el cluster Quito

Nombre CSS	**Partición (ordenadas en orden de prioridad)**	**Descripción**	**Tipo CSS**
CSS-Línea-Default	P-Block-Local P-Block-LD P-Block-INT	CSS a añadirse para cada línea que no tiene acceso a la PSTN, excepto el número de emergencia. Estas líneas corresponden a los teléfonos de recepción y de salas de estar	1
CSS-Línea-Local	P-Block-LD P-Block-INT	CSS a añadirse a líneas que pueden realizar llamadas locales y número de emergencia	1
CSS-Línea-LD	P-Block-INT	CSS a añadirse a líneas que pueden realizar acceder a la PSTN con excepción de llamadas internacionales	1
CSS-Línea-Managers	P-Manager-Interno	CSS a añadirse a líneas de asistentes	1
CSS-QU	P-Block	CSS a añadirse a	2

	P-Interna P-IPMA P-Emergencia-QU P-Local-QU P-LD-QU P-INT-QU	cualquier dispositivo en Quito	
CSS-CO	P-Block P-Interna P-IPMA P-Emergencia-CO P-Local-CO P-LD-CO P-INT-CO	CSS a añadirse a cualquier dispositivo en Coca	2
CSS-Restringido	P-Interna P-Block-Local P-Block-LD P-Block-INT	CSS que puede alcanzar únicamente la partición P-Interna. Será asignado a puertos CTI	3
CSS-AAR-CO	P-LD-AAR-CO P-INT-AAR-CO	CSS a asignarse para AAR en Coca	3
CSS-Gateway	P-Interna P-Manager-Interna P-IPMA	CSS a asignarse a los gateways para que alcancen los dispositivos para extender hacia las llamadas que vienen de la PSTN	3
CSS-taps	P-Autoregphone	Asignado en el nivel de arreglo de dispositivo. Este CSS es recibido para los teléfonos autoregistrados	1

- En el nivel de línea se debe asignar el CSS tipo 1 para cada línea dependiendo de la clase de servicio
- En el nivel de dispositivo se asigna el CSS tipo 2 para cada dispositivo dependiendo de la ubicación
- No asignar CSS para una línea que tiene un CoR no restringido

Cuando se define un CSS en ambos niveles, la lista de partición ubica en primer lugar a los niveles de línea y luego a los niveles de dispositivo. La Figura 40 ilustra cómo la combinación de ambos tipos resulta en un CSS que contiene todas las particiones de ambos niveles, en el que el bloqueo de las llamadas de larga distancia e internacionales se bloquean a pesar de la presencia de las

particiones que las permiten, ya que las particiones de bloqueo aparecen antes de las particiones que las admiten.

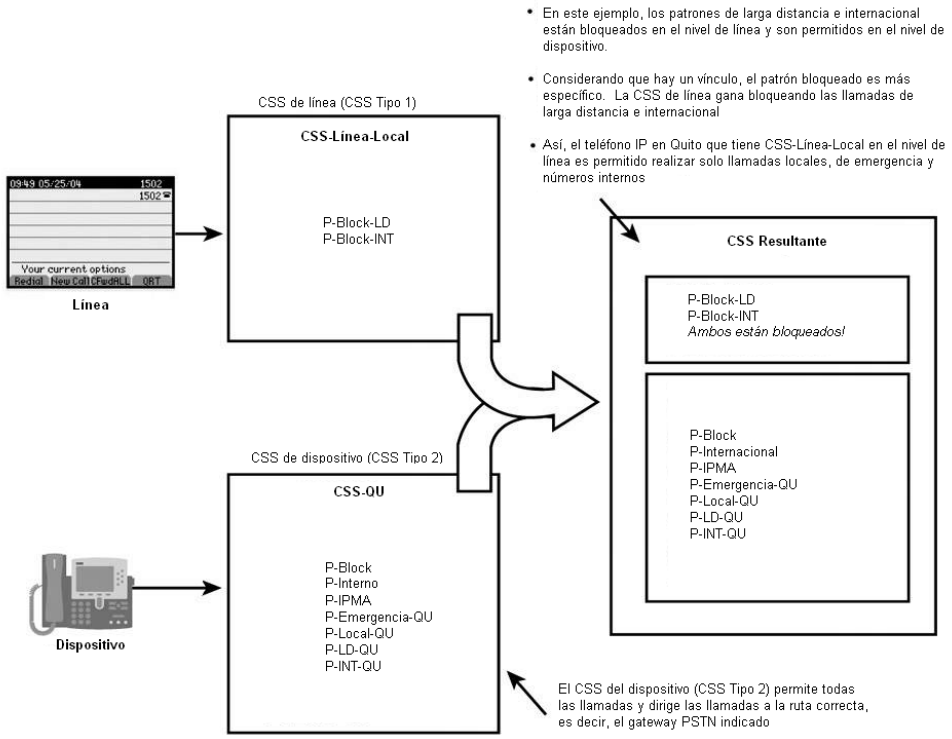

Figura 40. Ejemplo de CSS combinado

En el nivel de línea puede configurarse tres tipos de re-envío de llamadas: Re-envío de llamada por ocupado (Call Forward Busy, CFB), Re-envío de llamada por no Respondidas (Call Forward No Answer, CFNA) y Re-envío de todas las llamadas (Call Forward All, CFA). En las restricciones de CSS pueden aplicarse estas tres configuraciones. El CSS restringido permite únicamente llamadas

internas. El re-envío de una llamada hacia la PSTN estará permitido únicamente para los usuarios autorizados.

Un **grupo de ruta** es una lista priorizada de gateways al cual un modelo de ruta envía la llamada (por una lista de ruta). Determina el orden de preferencia para el uso de gateways y puertos. El Grupo de Ruta permite desbordamientos de llamadas hacia dispositivos alternos.

La Tabla LXXXI provee los detalles del grupo de ruta a crearse en el plan de discado de la red de las Fuerzas Armadas.

Tabla LXXXI. Grupos de ruta en el cluster Quito

Nombre de grupo	Orden de selección	Gateways/Dispositivos	Descripción
GR-GW-PSTN-QU	1	S1/DS1-0@QU-CMM1	Gateway para PSTN Quito
	2	S1/DS1-1@QU-CMM1	
	3	S1/DS1-0@QU-CMM2	
	4	S1/DS1-1@QU-CMM2	
GR-GW-INT-QU	1	S1/DS1-2@QU-CMM1	Llamadas internas en Quito
	2	S1/DS1-2@QU-CMM2	
GR-GW-PSTN-CO	1	S1/DS1-0@R3845-CO	Gateway para PSTN Coca
GR-Gatekeeper	1	Gatekeeper	ICTs entre los cluster Quito y cluster Guayaquil

Tabla LXXXII. Listas de ruta en el cluster Quito

Nombre de lista	Orden de selección	Grupos de ruta	Descripción
LR-PSTN-QU	1	GR-GW-PSTN-QU	Todas las llamadas PSTN que van por los troncos PSTN de Quito
LR-Interna-QU	1	GR-GW-INT-QU	Todas las llamadas internas en nodo Quito
LR-PSTN-no911-CO	1	GR-GW-PSTN-CO	Todas las llamadas PSTN que se originan desde Coca, excepto 911 y llamadas AAR
	2	GR-GW-PSTN-QU	
LR-PSTN-911-AAR-CO	1	GR-GW-PSTN-CO	Llamadas 911 y AAR realizadas desde Coca
LR-ICT-Guayaquil	1	GR-Gatekeeper	Llamadas ICT a Guayaquil realizadas desde cluster Quito
	2	GR-GW-PSTN-QU	
LR-ICT-Machala	1	GR-Gatekeeper	Llamadas ICT hacia Machala realizadas desde cluster Quito
	2	GR-GW-PSTN-QU	

Una **lista de ruta** define la manera en la que una llamada es enrutada. Las listas de ruta determinan el orden de preferencia de uso de un grupo de rutas. La configuración de una lista de ruta está asociada al menos con un grupo de rutas. La Tabla LXXXII muestra los detalles de las listas de ruta configuradas para el cluster Quito.

Los **modelos de ruta** brindan primordialmente las siguientes funciones:

- Asociar números discados para llamadas internas y externas
- Apuntar a una lista de ruta para el enrutamiento

La Figura 38 ilustra el modelo de ruta y su orden en la jerarquía de enrutamiento de llamada.

Antes de entrar al diseño del modelo de ruta para la red, se explican a continuación conceptos importantes respecto a los modelos de ruta, tales como wildcards, filtros de ruta, instrucciones de descarte de dígitos y transformaciones de dígitos.

En el CallManager, cada número de teléfono es un modelo de ruta. Es posible utilizar caracteres **wildcard** para definir los modelos de ruta que asocian un grupo de números discados. La Tabla LXXXIII muestra la lista de caracteres wildcard soportados por el CallManager y la Tabla LXXXIV muestra ejemplos de definiciones de los modelos de ruta utilizando caracteres wildcard.

Tabla LXXXIII. Caracteres wildcard

Wildcard	**Descripción**
0, 1, 2, 3, 4, 5, 6, 7, 8, 9, *, #	Asocia exactamente un dígito
x	Un solo dígito en el rango de 0-9
[x y z …]	Una ocurrencia de cualquier dígito en los corchetes
[x-y]	Una ocurrencia de cualquier dígito desde x a y
[^x-y]	Cualquier dígito que no esté entre x e y
!	Uno o más dígitos en el rango 0-9
Wildcard?	Cero o más ocurrencias del wildcard anterior
Wildcard+	Una o más ocurrencias del wildcard anterior
@	Asocia el plan de numeración nacional

Tabla LXXXIV. Ejemplos de modelos de ruta con caracteres wildcard

Definición de modelo de ruta	Descripción
2222	Asocia 2222
*2*2	Asocia *2*2
14xx	Asocia números entre 1400 y 1499
15[25-8]6	Asocia 1526, 1556, 1566, 1576, 1586
13[^3-9]6	Asocia 1306, 1316, 1326, 13*6, 13#6
13!#	Asocia cualquier número que empieza con 13, seguido de uno o más dígitos y termina con #, tal como 135# y 13579#

Entre los caracteres especiales mencionamos el . y @:

- . denota que una porción de un modelo de ruta puede ser sustraerse cuando el modelo coincide
- @ asocia el plan de numeración nacional o el plan de numeración que está instalado en el CallManager

Los **filtros de ruta** junto con los modelos de ruta utilizan cadenas de dígitos para determinar la forma en que se maneja una llamada. Los filtros de ruta son aplicables únicamente cuando se configura un modelo que contiene el wildcard @, en el que el CallManager enruta llamadas de acuerdo al plan de numeración registrado. Los filtros de ruta permiten determinar cuál modelo de ruta pueden los usuarios marcar.

Si se define un modelo de ruta 9.@ sin asociarse con un filtro de ruta, el CallManager chequea el número discado contra todos los modelos de ruta incluidos en el plan de discado. Por el contrario, la definición

de filtros de ruta permitirá seleccionar un número menor de modelos de ruta para que sean asociados al número marcado.

Luego de la definición de los elementos de un plan de ruta, es necesaria la configuración del proceso de **Transformación de dígitos** en el CallManager que consiste en la realización de modificaciones a los números de iniciación y de destinación de llamada antes de ser enviada al siguiente sistema. Están disponibles tres tipos de transformaciones de dígito:

- Transformaciones de la parte que llama
- Transformaciones de la parte conectada
- Transformaciones de la parte llamada

Estas transformaciones pueden realizarse en el CallManager en los siguientes niveles:

- Nivel de modelo de ruta
- Nivel de grupo de ruta dentro de una lista de ruta

Las transformaciones de dígitos realizadas en el nivel de grupo de ruta dentro de una lista de ruta se imponen a los definidos en el nivel de modelo de ruta. Realizaremos la manipulación de las transformaciones mediante el nivel de grupo de ruta ya que esta permite evitar errores de configuración.

La Figura 41 muestra las opciones disponibles para la transformación de dígitos en cada tipo en el **nivel de modelo de ruta**.

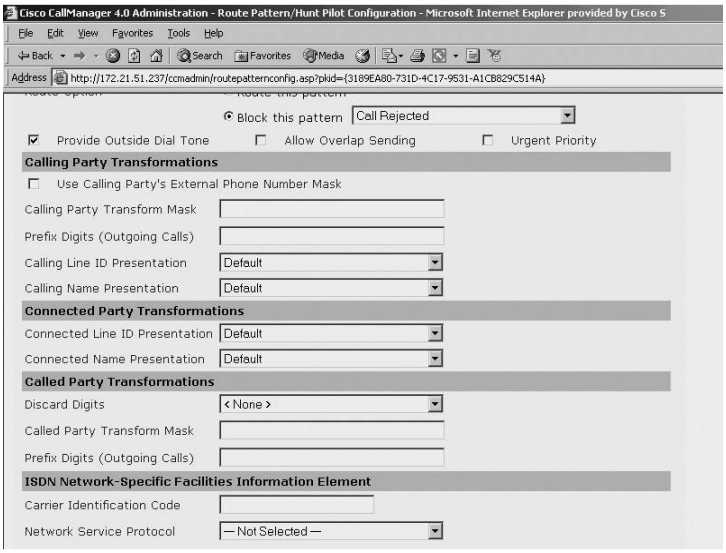

Figura 41. Transformaciones de dígito en el nivel de modelo de ruta

La Figura 42 muestra las opciones disponibles para la transformación de dígitos en cada tipo en el **nivel de grupo de ruta**.

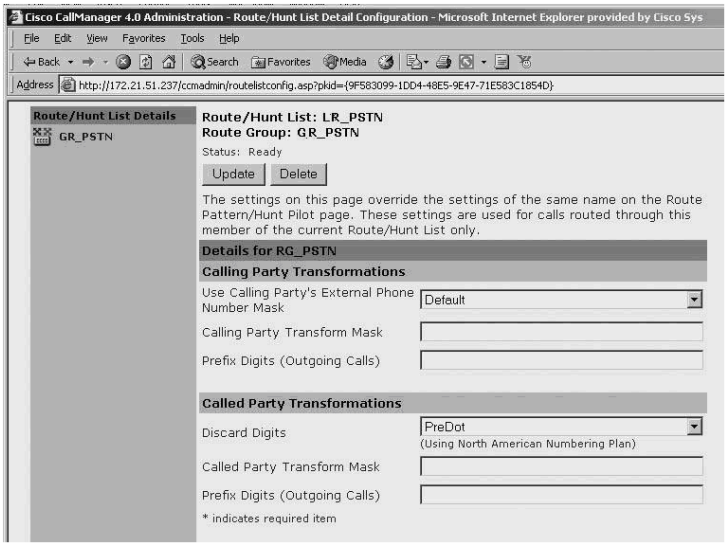

Figura 42. Transformaciones de dígito en el nivel de grupo de ruta

Las **transformaciones de la parte llamante** comprenden un cambio del ID de usuario. Se explican a continuación algunos parámetros de configuración:

- La señalación del casillero para “Use Calling Party’s External Phone Number Mask” indica al CallManager utilizar el valor del campo de la máscara de número externo de la página de configuración de directorio de números del teléfono IP que se muestra en la Figura 43. En esta página puede configurarse el campo que identifique el nombre de usuario del teléfono. La aplicación AAR utiliza el valor en el campo de máscara de número externo para enrutar la llamada por la PSTN. Si el campo no está seleccionado o está configurado con un número incorrecto, el AAR fallará.
- El campo “Calling Party Transform Mask” se utiliza para ocultar el número telefónico de la parte llamante antes de que la llamada sea enviada. Una máscara puede contener dígitos 0 a 9, *, x y #
- El campo “Prefix Digits” permite poner un prefijo al número llamante

En la red, cada nodo posee un número externo al cual podrán los usuarios de la PSTN comunicarse con los números de la red interna.

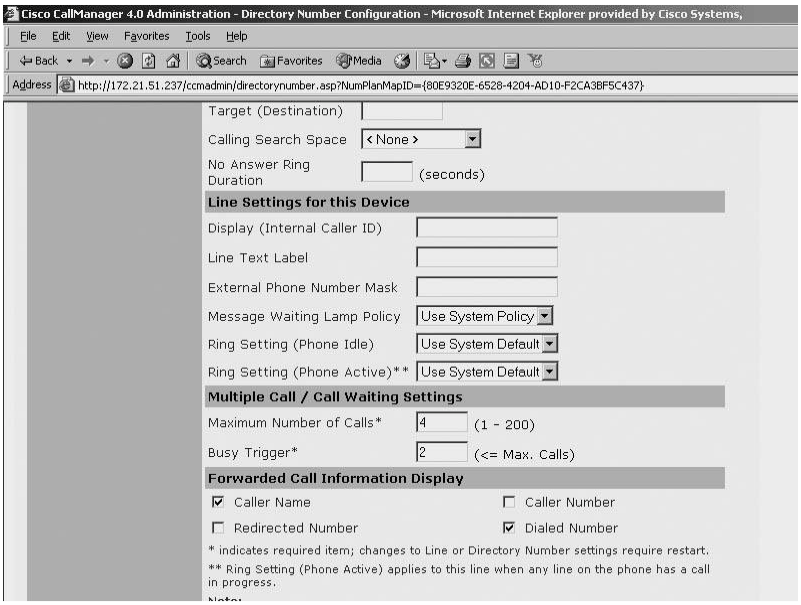

Figura 43. Transformaciones de la parte llamante en el nivel de número de directorio del teléfono

La Figura 41 muestra la sección de **Transformación de la parte conectada**, la misma que permite elegir si el CallManager permitirá o negará que se muestre el número de teléfono de la parte conectada en la pantalla del teléfono del usuario que llama.

Las Figuras 41 y 42 muestran las secciones respecto a la **Transformación de la parte llamada**. Estos campos contienen las mismas funcionalidades descritas en las Transformaciones de la parte llamante.

Un campo adicional mostrado en las Figuras 41 y 42 es **Discard Digits** cuyo valor permite modificar los dígitos del número llamado

antes de ser enrutado al siguiente sistema. Los DDIs (Digit Discarding Instruction, conjunto de reglas que permiten remover una parte de la cadena de dígitos marcados antes de que éste sea enviado al sistema siguiente) trabajan con modelos de ruta que son definidos utilizando el wildcard @, ubicado en el plan de discado.

La Tabla LXXXV ilustra la importancia de los DDIs. El número ubicado antes del punto (.) en cada modelo de ruta define el código de acceso, el mismo que definiremos con un valor de 9. El DDI para el modelo de ruta que comienza con 9. es **PreDot**, que quiere decir "Antes del punto". Con esto, el 9 será descartado y se enviará los números restantes al gateway especificado en la lista de ruta. Si el código de acceso no es parte del número telefónico, hay que descartar dicho número antes de ser enviado a la PSTN.

Como ya se mencionó antes, una razón para no recomendar la utilización de manipulación de dígitos en el nivel de modelo de ruta es por ejemplo cuando se digita un número 91408 y se ha fijado PreDot, el número almacenado en la lista de Llamadas Ubicadas en el teléfono IP es el número después del 9. Si el número es vuelto a marcar (redial), el 9 no estará incluido y la llamada no podrá completarse. Esta es la razón por la que la manipulación de dígitos debe realizarse en el nivel de grupo de ruta en vez del nivel de modelo de ruta.

Utilizaremos modelos de ruta específicos en lugar de emplear la macro @ con filtros de ruta.

Las Tablas LXXXV y LXXXVI describen los patrones de ruta definidos en la red de las Fuerzas Armadas.

Tabla LXXXV. Modelos de ruta del cluster Quito

Modelo de ruta	Partición	Lista de ruta	Descripción
5[0 1]XXX	P-Interna	LR-Interna-QU	Llamadas en el nodo Quito
5[2 3]XXX	P-Interna	LR-ICT-Guayaquil	Llamadas en la red a Guayaquil. Aplica máscara de transformación de parte llamada de 9042XXXXXX5[2 3]XXX en el GR-GW-PSTN-QU
5[4 5]XXX	P-Interna	LR-ICT-Machala	Llamadas en la red a Machala. Aplica la máscara de transformación de la parte llamada de 9072XXXXXX5[4 5]XXX en el GR-GW-PSTN-QU
9.911	P-Emergencia-QU	LR-PSTN-QU	911 para usuarios nodo Quito
9.911	P-Emergencia-CO	LR-PSTN-911-AAR-CO	911 para usuarios nodo Coca
9.2XXXXXX	P-Local-QU	LR-PSTN-QU	Llamadas locales en nodo Quito
9.2XXXXXX	P-Local-CO	LR-PSTN-911-AAR-CO	Llamadas locales en nodo Coca
9.[2-7]2XXXXXX	P-LD-QU	LR-PSTN-QU	LD para nodo Quito
9.[2-7]2XXXXXX	P-LD-CO	LR-PSTN-no911-CO	LD para nodo Coca
9.[2-7]2XXXXXX	P-LD-AAR-CO	LR-PSTN-911-AAR-CO	LD con AAR para Coca
9.011!	P-INT-QU	LR-PSTN-QU	Llamadas internacionales para nodo Quito

La Tabla LXXXVI muestra los modelos de ruta bloqueados para el cluster Quito.

Tabla LXXXVI. Modelos de ruta bloqueados para el cluster Quito

Modelo de ruta	**Partición**
9.2XXXXXX	P-Block-Local
9.[2-7]2XXXXXX	P-Block-LD
9.011!	P-Block-INT

6.2.3.2 Empleo del Gatekeeper en la Red De Fuerzas Armadas

Por definición un enlace troncal o troncos virtuales son aquellos que conectan dos o más clusters de CallManager. En este caso, para el control del número de llamadas a través de la ICT (en la WAN IP), podemos utilizar un Gatekeeper; para este caso, el protocolo a utilizarse para la comunicación entre el CallManager y el gatekeeper es H.323.

El empleo de un Gatekeeper que realice CAC en un CallManager requiere los siguientes pasos:

1. Seleccionar la plataforma de Hardware del Gatekeeper y el modo de despliegue
2. Configurar el Gatekeeper en el CallManager
3. Configurar el tronco en el CallManager
4. Configurar el Gatekeeper

Las ventajas de la utilización de un Gatekeeper en la comunicación entre clusters se definen a continuación:

- Escalabilidad, al reducir el número de ICTs requeridos para la comunicación entre clusters
- Facilidad de administración, al contar con la rápida adición y eliminación de rutas y dispositivos
- CAC entre las llamadas de clusters diferentes, asegurando que la asignación de anchura de banda de la WAN sea estrictamente cumplida
- Fácil configuración, al eliminar la necesidad de dispositivos extras H.323 para cada CallManager conectado a la WAN
- Capacidad para realizar enrutamiento de llamada básico en adición al CAC

El Gatekeeper es un software del Sistema operativo de los routers, por lo que la selección de la plataforma de hardware debe considerar algunos factores:

- Número de llamadas por segundo que el gatekeeper debe procesar
- Un modelo de despliegue que asigne al gatekeeper en modo clustering, que mejore el rendimiento y provea uso compartido de carga y redundancia en la red

La configuración del gatekeeper comienza con la **definición del gatekeeper** en el administrador del CallManager. La Tabla LXXXVII muestra los parámetros de configuración que se necesita ingresar para esta tarea.

Tabla LXXXVII. Parámetros de configuración del gatekeeper

Nombre del host/Dirección IP	Descripción	Tiempo de vida	Tiempo de espera para reintento de registro	Habilitar dispositivo
Dirección IP del GK	Gatekeeper	60	300	Habilitado

Luego de la configuración de la información del Gatekeeper, el siguiente paso es definir un tronco o enlace troncal desde el administrador del CallManager.

La Tabla LXXXVIII muestra los parámetros de configuración que debe ingresarse al definir un tronco de Gatekeeper en el CallManager.

Tabla LXXXVIII. Parámetros de configuración del tronco Gatekeeper

Parámetro	Valor
Información del dispositivo	
Nombre de dispositivo	AS_GKTrunk
Descripción	Tronco de Gatekeeper
Arreglo de dispositivos	DP-QUITO
MRGL	MRGL_QU
Ubicación	Quito
Grupo AAR	Ninguno
MTP requerido	No habilitado
Reintento de llamadas de video como audio	No habilitado
Información de enrutamiento de llamada – de entrada	

Dígitos significativos	Todos
Calling Search Space	CSS-Gateways
AAR Calling Search Space	
Prefijar DN	No
Redireccionar Número	Habilitado

- El MRGL, es una aplicación que permite al administrador localizar recursos de media en componentes
- Prefijar DN, prefijo que permite autenticar una llamada entrante para permitirle o negarle su paso al enlace troncal

6.2.3.3 Enrutamiento de llamadas entrantes

Las llamadas entrantes para Quito y Coca se receptan mediante el enlace troncal PRI. Los enlaces troncales PSTN en Quito terminan en puertos E1 PRI del CMM y en Coca terminan en puertos E1 PRI del Router. Los Gateways se configuran para utilizar MGCP. Estos Gateways reciben todos los dígitos de la PSTN, por lo que será necesario asignar el campo Attendant Directory Number para que pueda relacionar los números de directorio de un determinado número IP. Generalmente este número será el del teléfono IP del operador.

Otra configuración importante es el CSS. Para un exitoso enrutamiento de una llamada desde el Gateway al teléfono IP, el CSS en el Gateway debe incluir las particiones que contienen los teléfonos IP y los puntos de ruta CTI. Se debe fijar el campo CSS en el gateway a CSS-Gateway (Referencia Tabla LXXVIII).

6.2.3.4 Enrutamiento Automático Alternativo de llamadas

El AAR es un mecanismo que permite enrutar una llamada a la PSTN cuando el CAC niega la realización de la misma. AAR es una característica que se aplica solo dentro de un cluster, es decir, no funciona entre dos clusters de CallManager.

Los pasos para configurar AAR son:

1. Habilitar el parámetro de servicio AAR
2. Definir la máscara de número telefónico externo
3. Configurar los grupos AAR y asignar los números de directorio de los teléfonos IP y gateways al grupo AAR
4. Definir CSSs para AAR y asignarlos a los teléfonos IP y gateways

El primer paso para configurar AAR es habilitar éste en el administrador del CallManager, fijándolo en un valor “TRUE”.

El CallManager reconoce el número que debe marcar para que alcance un número en otro sitio mediante el uso de la PSTN cuando el CAC ha bloqueado el enrutamiento de la llamada por la IP WAN mediante una referencia al campo de Máscara Telefónica Externa en el directorio de configuración de números del directorio. En la Tabla LXXXIX se muestra la máscara del número telefónico externo para cada ubicación de la red telefónica de las Fuerzas Armadas:

Tabla LXXXIX. Máscara telefónica externa aplicada al nivel de línea

Sitio	Máscara externa de número de teléfono
Quito	2XXXXX1
Guayaquil	2XXXXX2
Coca	2XXXXX3
Machala	2XXXXX4

Otra pregunta importante que hay que resolver es cómo el CallManager conoce el código de acceso que se debe discar para alcanzar la PSTN. La respuesta se encuentra en los grupos AAR. Un grupo AAR especifica el código de acceso que necesita ser añadido a la máscara del número telefónico externo antes de hacer la llamada hacia la PSTN.

El paso final en la configuración del AAR es definir los CSSs para los AAR y asignarlo en los niveles de dispositivo para gateways y para los teléfonos IP. Estos ya han sido definidos en la Tabla LXXX.

6.2.4 TELEFONÍA DE SUPERVIVENCIA PARA SITIOS REMOTOS

Survivable Remote Site Telephony SRST provee al CallManager un recurso de emergencia para los teléfonos IP que están conectados a los routers de la Ethernet local. El SRST permite a los routers proveer un soporte de manejo de llamada para los teléfonos, cuando éstos pierden conexión al CallManager primario, secundario o terciario o cuando la conexión WAN se cae.

El SRST se despliega para cada sitio remoto de la red en los clusters de Quito y Guayaquil.

Bajo el modo SRST, los usuarios de los teléfonos IP no pueden utilizar los cinco dígitos para marcar a otros teléfonos de un sitio diferente.

6.2.5 SERVICIOS DE FAX Y MODEM EN LA RED IPT

Para el despliegue de los servicios de FAX y MODEM se aplicará el mecanismo de fax y MODEM pass-through. Con este mecanismo, el CODEC a utilizarse debe ser el G.711. Debido a limitaciones del CallManager, el modo pass-through no podrá utilizar su característica up-speed que permite el uso de codecs de alta compresión (G.729) para las llamadas de voz, ya que el mecanismo CAC no puede ajustar el ancho de banda deducido. Todos los terminales de fax y MODEM pertenecerán al arreglo de dispositivos DP-FAX. Esto obligará que una llamada sea negociada como una llamada G.711 y asigne el ancho de banda apropiado por el CAC.

En la red de las Fuerzas Armadas en los nodos de Quito y Guayaquil, las llamadas de fax entrantes de la PSTN viene de los gateways WS-SVC-CMM-6E1. Los faxes se conectan a los gateways VG248. En los sitios remotos, las llamadas de fax entrantes llegan al gateway MGCP.

La Figura 44 muestra la configuración en el gateway WS-SVC-CMM-6E1 del Catalyst.

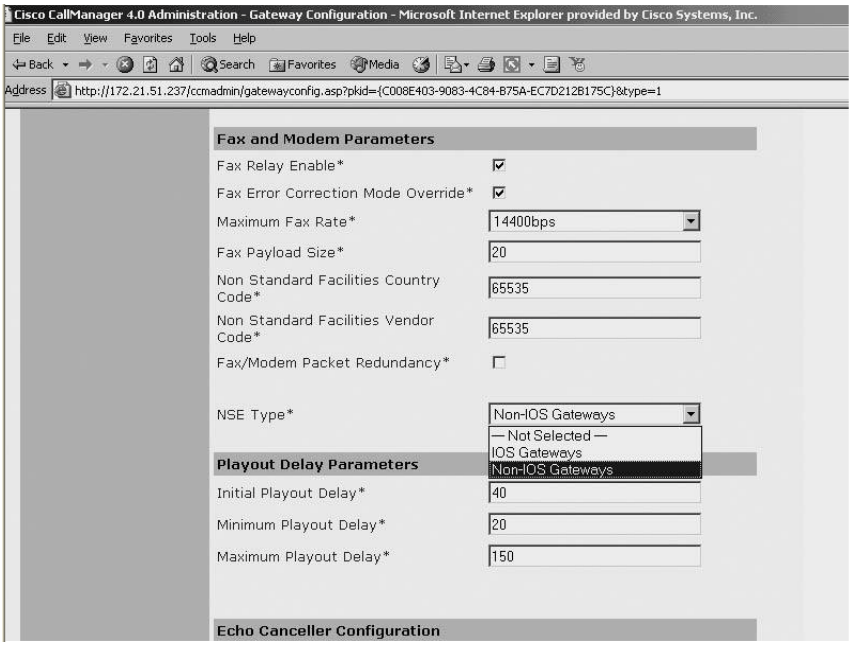

Figura 44. Configuración Fax pass-through en el gateway WS-SVC-CMM-6E1 del Catalyst

La Figura 45 muestra la configuración del VG248, que es un gateway basado en SCCP para la habilitación de fax pass-through. En la configuración del VG248 debe observarse lo siguiente:

- El VG248 puede negociar pass-through, si el fax relay (método de transporte de datos de fax en la red IP en vez de enviarla como información de voz) está habilitado en el VG248 y el gateway far-end soporta solo fax pass-through,
- Deshabilitar la llamada en espera en el puerto destinado a fax

- El VG248 es compatible con dispositivos antiguos. Es necesario cambiar el parámetro de señalización pass-through al modo IOS (Referencia Figura 43). Se debe mantener la señalización pass-through en modo IOS a través de la red en todas las configuraciones de gateways (que no soportan IOS), en caso de que todos los otros gateways estén basados en IOS, los mismos que son VG248.

Cisco VG248 (VGC10101010AA)	
Advanced settings	
Allow last good configuration	(enabled)
SRST policy	(disabled)
SRST provider	( )
Call preservation	(enabled: no timeout)
Media receive timeout	(disabled)
Busy out of hook ports	(disabled)
DTMF tone duration	(default: 100ms)
Echo cancelling policy	(alternate: use DSP)
Passthrough signalling	**(IOS mode)**
Hook flash timer	(<country default>)
Hook flash reject period	(none)
Fax relay maximum speed	(default: 14400 bps)
Fax relay playout delay	(default: 300)

Figura 45. VG248 - Gateway SCCP

6.2.6 SEGURIDAD DE LA INFRAESTRUCTURA DE LA IPT

La seguridad en la red de las Fuerzas Armadas se tomará en cada capa y en cada componente diferente de la red, como muestra la Figura 46. Con este método por capa, si la seguridad se ve comprometida, el problema se ubicaría en un solo nivel.

A continuación se examinan los componentes de la red y las medidas de seguridad que deben implementarse:

- Seguridad en el CallManager y servidores de aplicación

- Utilización de firewalls y listas de control de acceso ACLs
- Seguridad de la red IPT del mundo exterior
- Seguridad de los terminales IPT
- Seguridad de los dispositivos de la red
- Seguridad de los gateways de voz
- Establecimiento de seguridad física
- Instalación de detección de intrusos a hosts

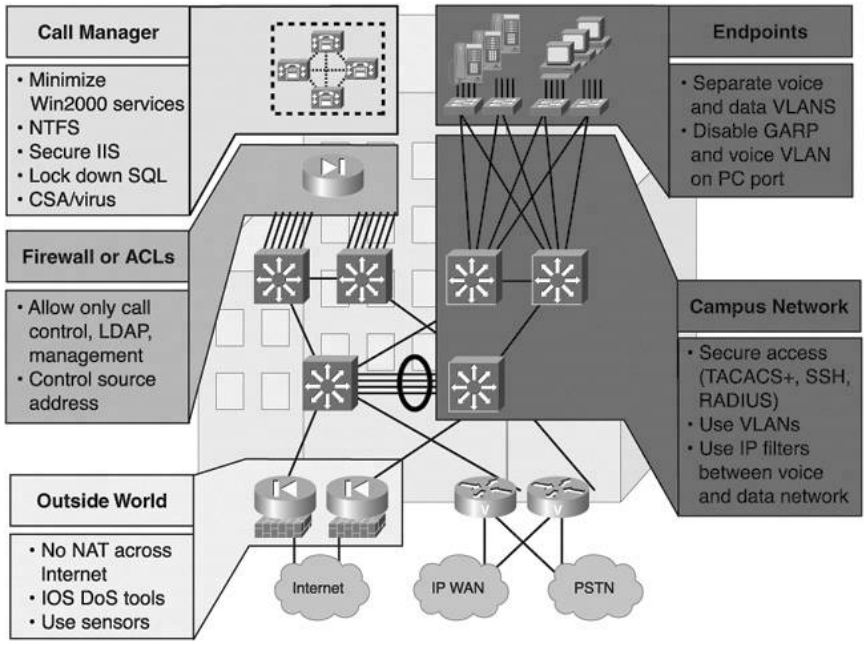

Figura 46. Infraestructura IPT de seguridad multicapa

En el **CallManager y servidores de aplicación** será posible asegurar el sistema operativo del CallManager deshabilitando los servicios de información de Internet de los suscriptores y los servicios de Windows que no son utilizados, etc.

El CallManager cuenta con un script de seguridad, el mismo que cuando es ejecutado, se ponen en funcionamiento comandos predefinidos para realizar tareas de seguridad para el sistema operativo. Además es importante realizar las actualizaciones del CallManager y otras aplicaciones de los servidores de forma periódica.

El CallManager no cuenta con un antivirus propio. Será necesaria la utilización de un producto como Mc Afee o Norton Antivirus que son soportados por la plataforma y otros servidores, los mismos que podrán ser programados para ejecutarse en horas no pico.

Es prudente ubicar los clusters de CallManager en diferentes VLANs y redes, de forma que si un ataque de virus o un DoS ocurriera en la red, solo afecte a los servidores de dicha red.

La **utilización de firewalls y ACLs** en el CallManager y en los servidores IPT añade una capa adicional de seguridad. Las ACLs se configuran para permitir que solamente tráfico conocido pueda acceder a los servidores en el cluster de CallManager. Las ACLs deben ubicarse en las interfases adecuadas para que puedan realizar un filtrado eficiente de los usuarios que ingresan a la red.
Cuando se ubica un firewall frente a la red de voz es necesario asegurarse de que soporta una inspección a tiempo completo de los protocolos de señalización de voz. El firewall habilita únicamente los puertos UDP

configurados para el tráfico de voz. El firewall a utilizarse debe soportar capacidades de Gateway de Capa de Aplicación (Application Layer Gateway, ALG). ALG inspecciona los paquetes de señalización para descubrir qué puertos UDP utiliza los flujos RTP y dinámicamente abre un paso para dicho puerto UDP.

Para **asegurar la red del mundo exterior**, es recomendable no utilizar Traducción de Dirección de Red (Network Address Translation, NAT) para una red privada. Por el contrario, se recomienda utilizar un servidor Proxy para alcanzar el Internet, evitando así que el CallManager llegue al Internet directamente.

Con el fin de proteger a los distintos servidores, es necesario tomar ciertos pasos para dar **seguridad a los terminales IPT**. Es importante aislar las redes de voz y de datos mediante el uso de VLANs, ya que además de permitir una mejor administración de ambos servicios, ayuda a incrementar la seguridad de la red de voz.

Hay muchas características de seguridad disponibles para proteger los teléfonos IP.

- Gratuitous ARP (GARP): Los dispositivos utilizan GARP para anunciar su presencia en la red. Sin embargo, los atacantes pueden utilizar éste para burlar un dispositivo válido de la red. Deshabilitar esta opción permitirá que los teléfonos ignoren los paquetes GARP

- Acceso a VLAN de voz: Los teléfonos IP tiene la capacidad de pasar todos los paquetes de voz recibidos en el puerto del switch al puerto PC. Se deberá deshabilitar esta opción para detener el envío de paquetes al puerto PC y con ello prevenir la entrada y salida de paquetes de datos en la VLAN de voz
- Puerto PC: Es recomendable deshabilitar el puerto PC de los teléfonos IP en áreas comunes como salas de espera y lobby
- Acceso de configuración: La deshabilitación de este campo previene que los usuarios puedan ver o modificar las configuraciones de la red en los teléfonos IP

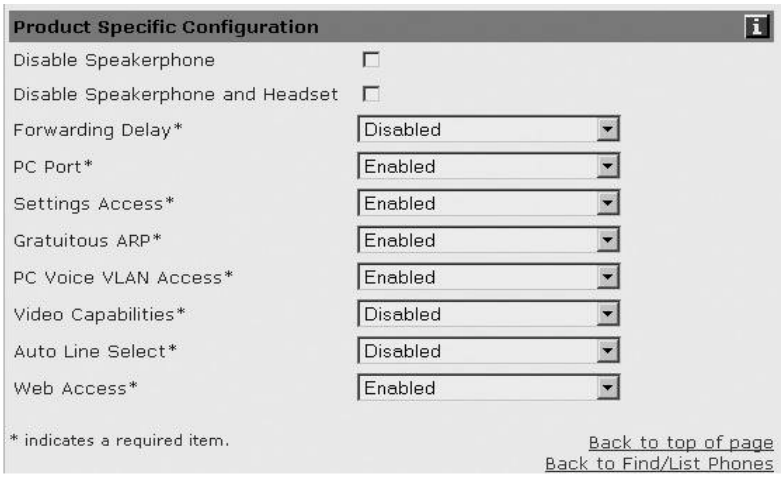

Figura 47. Configuraciones específicas a los teléfonos IP

La **seguridad en los dispositivos de la red** como switches y routers puede brindarse utilizando métodos de autenticación como TACACS+ y RADIUS. Esta configuración puede realizarse desde el CLI mediante sesiones Telnet. Es también muy importante deshabilitar los puertos en los switches que no se utilizan y ubicarlos en VLANs no usados.

La **seguridad en los gateways de voz** puede incrementarse mediante la aceptación de mensajes de control de VoIP únicamente de servidores CallManager reconocidos por el cluster. Los gateways deberán denegar las conexiones H.323, MGCP, Skinny o SIP que atenten a la red de datos.

Generalmente no existe un control en la **seguridad física de la red**. Los equipos de red deberían mantenerse bajo condiciones ambientales adecuadas.

Es importante contar con una **aplicación para detección de intrusos a hosts** con el fin de prevenir actividades maliciosas e indeseadas en los hosts. Estas aplicaciones detectan y bloquean acciones perjudiciales, independientes de los ataques.

6.3 DISEÑO INTEGRAL DE LA RED DE TELEFONÍA IP EN LA RED DE DATOS DE LAS FUERZAS ARMADAS

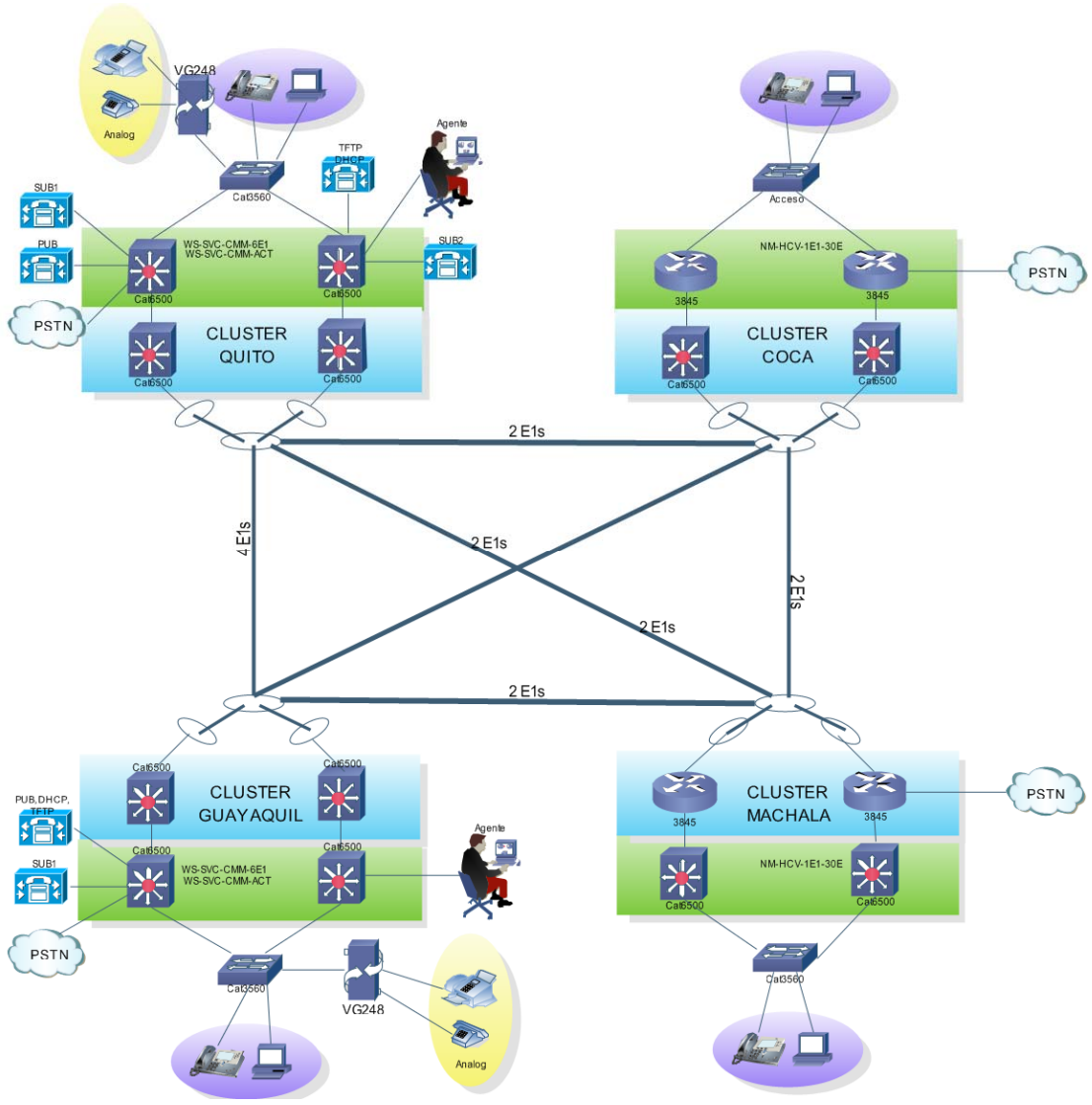

Figura 48. Diseño Integral de la Red de telefonía IP en la red de datos de las Fuerzas Armadas

Capa	Equipo	Nodos			
		Quito	Guayaquil	Coca	Machala
Wan	Switch-Router Catalyst 6500	2	2	2	2
Distribución	Switch-Router Catalyst 6500 y tarjeta Gateway WS-SVC-CMM-6E1	2	2	0	0
	Router 3845 y tarjeta Gateway NM-HDV-1E1-30E	0	0	2	2
	Plataforma MCS-7835 (CallManager 3.3)	1	1	0	0
Acceso	Catalyst 3560/48	25	32	10	10
	VG-248	1	1	0	0
	Teléfono 7940	164	155	32	32
	Teléfono 7936	7	6	1	1
	Teléfono 7905	726	1148	320	320
	Fax	25	20	0	0

El diseño de red que hemos analizado detalladamente y es el propuesto para la red de datos de las Fuerzas Armadas tiene las siguientes características:

1. La arquitectura de Procesamiento de Llamada es Centralizado, en el cual se desplegarán dos CallManager Cluster cuyas aplicaciones estarán localizadas en los dos nodos más importantes (Quito y Guayaquil) y serán éstos quienes darán asistencia a los dos nodos restantes.
2. En QUITO tendremos un Call Manager Cluster y un servidor DHCP que también cumplirá el servicio TFTP; mientras que en Guayaquil, el Call Manager Publisher dará el servicio DHCP y el servicio TFTP.

3. Con respecto a la red WAN, la decisión de las Fuerzas Armadas es mantener el existente enlace PDH.
4. Con respecto a la enlace físico, se utilizarán switches Catalyst 3560 en las capas de acceso y Catalyst 6500 en las capas de distribución y de núcleo; todos con características QoS.
5. Se crearon las respectivas VLANs con su identificador. La asignación de direcciones IP se realizó mediante el servicio DHCP.
6. En el análisis de diseño de **alto nivel**, se cubrieron los requerimientos de fax, teléfonos analógicos y módems, gracias al equipo VG248. También se da la opción de conferencias multipunto, y de operador automático.
7. En el análisis de diseño de **bajo nivel**, se determinó la presencia de dos Call Manager Cluster, con un número específico de servidores, ubicados en Quito y Guayaquil.
8. En los Call Manager se detalló los pasos a seguir para la configuración de auto-registro, fecha y hora, región y ubicación, arreglo de dispositivos, recursos de media, etc.
9. Con respecto a la **arquitectura de discado**, el plan de numeración interna será de 5 dígitos; y mediante el empleo de modelo, lista y grupo de rutas se realizará el enrutamiento de las llamadas.
10. Tomando como base el modelo de cálculo Erlang B y Erlang C, se logró determinar que 5 sería el número mínimo de puertos IVR y 2 el número mínimo de operadores.
11. Gracias al empleo de un gatekeeper en la comunicación entre clusters se logrará: escalabilidad y facilidad de administración.

12. En lo que respecta a las llamadas entrantes para Quito y Coca se receptarán mediante el enlace troncal PRI. Los enlaces troncales PSTN en Quito terminarán en puertos E1 PRI del CMM y en Coca terminarán en puertos E1 PRI del Router.
13. Se emplearán Gateways (configurados para utilizar MGCP), que reciban todos los dígitos de la PSTN
14. Mediante el empleo de el AAR, lograremos enrutar una llamada para a la PSTN cuando el CAC niegue la realización de la misma.
15. Con todo el trabajo realizado en esta tesis, obtendremos un moderno diseño de una red de telefonía IP, con una proyección de servicio calculada para 6000 usuarios, empleando 2912 teléfonos.

CONCLUSIONES Y RECOMENDACIONES

1. La descripción de las tendencias mundiales telefónicas y la situación de la misma en el Ecuador, permite concluir que se debe realizar un estudio profundo de las debilidades del sistema telefónico existente, así como la elaboración de un proyecto que permita tener comunicaciones IP en el Ecuador.
2. Las comunicaciones de Fuerzas Armadas representan una parte importante y sensible de la Seguridad Nacional, por lo que su desarrollo y evolución a IP, permite obtener mayor flexibilidad.
3. Los estudios realizados en la fase de planificación de este diseño telefónico IP, permiten ejecutar los trabajos de una forma eficiente.
4. Los avances que se han presentado en las redes de Comunicaciones, y en especial de Telefonía, permiten el empleo de Telefonia IP tanto en Redes administrativas, como en Redes Operativas.
5. En el desarrollo de la tesis se presentaron algunas alternativas de cada uno de los protocolos existentes y empleados en telefonía IP, permitiéndonos hacer un análisis adecuado para la mejor selección del mismo.
6. No existe un entorno común de creación de servicios para las redes de siguiente generación. Cada arquitectura estudiada aplicada a una situación en especial, permite brindar las bondades y el rendimiento esperado en función de los recursos asignados.
7. El auge de la telefonía IP es algo evidente y la principal razón es el reaprovechamiento de los recursos y la disminución en el coste de llamadas.

Sin embargo, si de algo adolece todavía la VoIP es de la calidad de los sistemas telefónicos tradicionales. Ante aquello es importante el control permanente de la red diseñada que permita disminuir los tiempos de latencia. Cuanto mejor conozcamos los problemas que se producen y sus posibles soluciones mayor calidad disfrutaremos.

8. Dentro de la organización militar, lugar donde se aplicará el diseño propuesto, hay que satisfacer las necesidades de comunicación de datos y voz. Hasta la aparición de la telefonía IP no había una solución unificada, lo que implicaba tener una red para los datos y otra para las comunicaciones telefónicas. La aparición de esta nueva tecnología permite integrar la telefonía dentro de la red de datos. Esto supone un mantenimiento más sencillo puesto que solo hay una infraestructura común.
9. En una red militar, que debe gozar de alta confiablidad, fue necesaria la implementación de equipos redundantes que permitan la subsistencia de las comunicaciones ante cualquier problema que repercuta en ambas funciones (voz y datos).
10. El uso de la misma red para datos y voz supone a su vez la reducción en los costes. Las llamadas dentro de cada una de las unidades militares no tienen coste, generando un ahorro de dinero a las Fuerzas Armadas.
11. Las ventajas que ofrece VoIP son suficientes para planteare su uso dentro de una organización. Incluso los problemas de ruido que inicialmente planteaba esta tecnología han sido mejorados, consiguiéndose una alta calidad en la comunicación. Sin embargo, no todo son ventajas.

12. En nuestro diseño no se han considerado mayores seguridades para la red IPT debido a que el empleo que se le da en estos momentos en las Fuerzas Armadas es de carácter administrativo. En caso que el órgano administrador de la red desee emplear este medio de comunicación para el envío de información calificada, se deberá proceder al empleo de equipos criptográficos o realizar algún tipo de encripción. Cabe señalar que las Fuerzas Armadas emplean otro medio para comunicaciones de carácter reservado.

ANEXOS

Cisco 3800 Series Integrated Services Routers

http://www.cisco.com/en/US/prod/collateral/routers/ps5855/product_data_sheet0900aecd8016a8e8.pdf

Cisco Catalyst 6500 Series and Cisco 7600 Series Communication Media Module

http://www.cisco.com/en/US/prod/collateral/switches/ps5718/ps708/product_data_sheet0900aecd8066426f.pdf

Understanding High Density Voice Network Modules

http://www.cisco.con/en/US/tech/tk652/tk701/technologies_tech_note09186a00800b65d6.shtml

Cisco CallManager Version 3.3

http://www.cisco.com/warp/public/cc/pd/nemnsw/callmn/prodlit/cm33_ds.pdf